CYBERSECURITY: AN EXAMINATION OF THE COMMUNICATIONS SUPPLY CHAIN

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MAY 21, 2013

Serial No. 113–46

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
85–436 WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

RALPH M. HALL, Texas
JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Missouri
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
FRANK PALLONE, Jr., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY McNERNEY, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

GREG WALDEN, Oregon
Chairman

ROBERT E. LATTA, Ohio
Vice Chairman
JOHN SHIMKUS, Illinois
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
MARSHA BLACKBURN, Tennessee
STEVE SCALISE, Louisiana
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
JOE BARTON, Texas
FRED UPTON, Michigan, *ex officio*

ANNA G. ESHOO, California
Ranking Member
EDWARD J. MARKEY, Massachusetts
MICHAEL F. DOYLE, Pennsylvania
DORIS O. MATSUI, California
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
JOHN D. DINGELL, Michigan
FRANK PALLONE, JR., NEW JERSEY
BOBBY L. RUSH, Illinois
DIANA DeGETTE, Colorado
JIM MATHESON, Utah
HENRY A. WAXMAN, California, *ex officio*

CONTENTS

Page

Witnesses

CYBERSECURITY: AN EXAMINATION OF THE COMMUNICATIONS SUPPLY CHAIN

TUESDAY, MAY 21, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:02 p.m., in room 2123 of the Rayburn House Office Building, Hon. Greg Walden (chairman of the subcommittee) presiding.

Members present: Representatives Walden, Latta, Shimkus, Terry, Blackburn, Lance, Guthrie, Gardner, Long, Ellmers, Eshoo, Matsui, Welch, and Waxman (ex officio).

Staff present: Carl Anderson, Counsel, Oversight; Ray Baum, Senior Policy Advisor/Director of Coalitions; Neil Fried, Chief Counsel, C&T; Debbee Hancock, Press Secretary; David Redl, Counsel, Telecom; Charlotte Savercool, Executive Assistant, Legislative Clerk; Kelsey Guyselman, Telecom; Roger Sherman, Democratic Chief Counsel; Shawn Chang, Democratic Senior Counsel; Margaret McCarthy, Democratic Staff; Patrick Donovan, Democratic FCC Detail; and Kara Van Stralen, Democratic Policy Analyst.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. We are going to call to order the Subcommittee on Communications and Technology for our hearing on “Cybersecurity: an Examination of the Communications Supply Chain.” And just for the benefit of our witnesses—I don’t know if benefit is the right word—but in about 10 minutes we are probably going to get called to the House Floor for votes. So don’t flee when we do. We will plan to return and be sure and get your testimony in and our questions. But we will begin with our opening statements and, as you know, things around here aren’t always certain so, who knows, we may get everything done, but I doubt it. So we will go ahead and get started, but we want to thank you all for being here and for submitting your testimony.

Our communications networks strengths—its ubiquity and interconnected nature—may actually also be a weakness. Those who wish to harm our Nation, to steal money or intellectual property, or merely to cause mischief can focus on myriad hardware and software components that make up the communications infrastructure. And they can do so anywhere in the design, the delivery, the installation, or the operation of those components. So today's hearing will focus on securing that communications supply chain.

We are fortunate to have as a member of this subcommittee the full chairman of the House Intelligence Committee, Chairman Mike Rogers. The experience and resources he brings were invaluable to the bipartisan Cyber Security Working Group last Congress, as well as to this subcommittee's three prior cyber hearings.

Many of us have concluded that promoting information-sharing through the Cyber Intelligence Sharing and Protection Act, CISPA, that he and Representative Ruppersberger have now twice assured through the House with large bipartisan votes, is pivotal to better securing our networks. It was also in large part this committee's 2012 report on the communications supply chain that prompted this hearing. Supply chain risk management is essential if we are to guard against those that would compromise network equipment or exploit the software that runs over and through it.

Understanding that you can never eliminate these risks, how do you minimize them without compromising the interconnectivity that makes networks useful? How secure is the communications supply chain? Where are the vulnerabilities? How much should we focus on securing physical access to components as they make their way from design to installation? How much on the internal workings of the components themselves? How do the risks and responses differ for hardware and software? What about for internationally sourced products as opposed to domestically sourced products? What progress has been made through the public-private partnerships, standards organization, and the development of best practices, and what role should the government play?

These are among the questions we will examine in this hearing, as well as through the bipartisan Supply Chain Working Group that we launch today. Representative Mike Rogers and my colleague and friend from California, Anna Eshoo, will co-chair this group, which will also include Representatives Latta, Doyle, Terry, Lujan, Kinzinger, and Matheson.

As I did last Congress, I will urge that we abide by a cyber Hippocratic Oath and first do no harm as we consider the tools available to the public and private sectors in making our communications supply chain secure.

With that, I would yield to the vice chair of the subcommittee, Mr. Latta.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Our communications network's strengths—its ubiquity and interconnected nature—may also be weaknesses. Those who wish to harm our nation, to steal money or intellectual property, or merely to cause mischief, can focus on myriad hardware and software components that make up the communications infrastructure. And they can do so anywhere in the design, delivery, installation or operation of those components. Today's hearing will focus on securing that communications supply chain.

We are fortunate to have as a member of this subcommittee House Intelligence Committee Chairman Mike Rogers. The experience and resources he brings were invaluable to the bipartisan cybersecurity working group last Congress as well as this subcommittee's three prior cyber hearings. Many of us have concluded that promoting information sharing through the Cyber Intelligence Sharing and Protection Act that he and Rep. Ruppersberger have now twice ushered through the House is pivotal to better securing our networks. It was also in large part his committee's 2012 report on the communications supply chain that prompted this hearing. Supply chain risk management is essential if we are to guard against those that would compromise network equipment or exploit the software that runs over and through it.

Understanding that you can never eliminate these risks, how do you minimize them without compromising the interconnectivity that makes networks useful? How secure is the communications supply chain? Where are the vulnerabilities? How much should we focus on securing physical access to components as they make their way from design to installation? How much on the internal workings of the components themselves? How do the risks and responses differ for hardware and software? What about for internationally sourced products as opposed to domestic ones? What progress has been made through public-private partnerships, standards organizations and the development of best practices? What role should the government play?

These are among the questions we will examine in this hearing, as well as through the bipartisan supply chain working group we launch today. Reps. Mike Rogers and Anna Eshoo will co-chair the group, which will also include Reps. Latta, Doyle, Terry, Lujan, Kinzinger, and Matheson. As I did last Congress, I will urge that we abide by a cyber Hippocratic Oath and first do no harm as we consider the tools available to the public and private sectors in making our communications supply chain secure.

# \# \#

Mr. LATTA. Thank you, Mr. Chairman, and I appreciate you yielding and holding this hearing today on a very critical and important topic. I want to thank our witnesses for being here and I look forward to your testimony today.

Not a day goes by that I don't seem to pick up a newspaper and read about a cyber attack or the vulnerability on the front page of a newspaper. Cyber crime and cyber warfare can affect any individual or business since we all depend on our interconnected communication networks. This is an issue not just of national security but economic security.

Again, I thank our witnesses for being here. I look forward to your comments on the communications supply chain. I also thank the Chairman for convening a bipartisan working group on this topic and I look forward to being part of the start of a very thoughtful and serious discussion on the threats of the supply chain and possible solutions. And with that, Mr. Chairman, I yield back.

Mr. WALDEN. Anyone else on the Republican side seeking to make a comment on the final minute-and-a-half of my time? If not, I yield back the balance and recognize my friend, the ranking member of this subcommittee, Ms. Eshoo, for 5 minutes.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Thank you, Mr. Chairman, and thank you for holding this very important hearing. Welcome to all of our witnesses.

Mr. Chairman, the implications of foreign-controlled telecommunications infrastructure companies providing equipment to the U.S. market, I think, really presents a very real threat to our country. As the Office of the National Counterintelligence Executive has noted, "the globalization of the world economy has placed critical links in the manufacturing supply chain under the direct control of U.S. adversaries."

Just last month, despite press reports suggesting that Huawei was leaving the U.S. market, the company now denies such reports and has stated that, “Huawei has no connection to the cyber security issues the U.S. has encountered in the past, current, and future.” That is quite a statement.

These are not new threats. It in fact, more than 3 years ago as a member of the House Intelligence Committee, I wrote to the director of National Intelligence asking for an assessment of the national security implications of Chinese-origin telecommunications equipment on our law enforcement and intelligence efforts, as well as on our switch telecommunications infrastructure. While I can’t discuss, obviously, the results of that assessment in an unclassified hearing, suffice it to say, the answers were troubling.

Since that time, I have reiterated my concerns with the FCC Chairman Genachowski and in late 2011 I joined colleagues in requesting that the GAO study the potential security risks of foreign manufactured equipment. The newly released GAO study recognizes that multiple points within the supply chain can create vulnerabilities for threat actors to exploit. But a combination of initiatives by both the public and private sector are being established to fight back.

The President’s Executive Order issued in February is an example. NIST has been tasked with developing a framework to reduce cyber attacks to critical infrastructure, and as NIST undertakes the development of this framework, supply chain security should be a component. In fact, this morning, Chairman Walden and myself raised this very issue with Dr. Gallagher.

Moving forward, I am very pleased to co-chair, at the chairman’s request, the subcommittee’s newest working group focusing on supply chain security and integrity with Representative Mike Rogers, who chairs the House Intelligence Committee. And through stakeholder meetings, I think we will be able to better understand what additional steps can be taken to protect U.S. telecommunications infrastructure from inappropriate foreign control or influence.

So again, I thank each one of our witnesses that are here today for your important testimony that you are going to give, the important answers that you are going to give to our questions, and for your steadfast commitment to securing the communications equipment supply chain for our Nation.

And I yield back, Mr. Chairman.

Mr. WALDEN. If you want to yield to——

Ms. ESHOO. Does anyone want me to yield my remaining time to them? Ms. Matsui or—OK. Sure.

Ms. MATSUI. Thank you very much, Ms. Eshoo. I would like to also thank the chairman for holding today’s hearing.

This year alone, we have seen significant cyber breaches to our economy. We know rogue states and skilled hackers are relentless and continue to pose a real threat breaching sensitive information stored by both the private and public sectors, as well as the American consumer.

To address the cyber threats I believe industry and government must be partners. It is not a one-way street. We live in a digital world where information is readily available on the internet and can be accessed from just about anywhere. We also live in an innovative economy where America's innovative spirit has led to new devices, equipment, and communications that penetrate the global marketplace.

This has also created an international supply chain of technology components. Today, it is not surprising if a product and its components originate from several different countries. That is why it is critical for industry to continue to be vigilant in assuring their manufacturing and distribution processes are not compromised. We should also be mindful of hackers trying to circumvent the supply chain by infecting botnets and malware onto popular mobile apps.

Addressing mobile security should be a priority moving forward, particularly as millions of Americans download their favorite apps, which in some cases includes personal information.

Again, I thank the chairman for holding today's hearing and I yield back the remainder of my time.

Mr. WALDEN. The gentlelady yields back the remainder of her time. And seeing no one on our side seeking time, I would yield now to the gentleman from California, Mr. Waxman, for 5 minutes.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you very much, Mr. Chairman, for holding today's hearing on cyber security risks in the communications supply chain.

This morning, our full committee heard a wide range of perspectives on the cyber threats to our critical infrastructure, including broadband networks.

While the Executive Order on cyber security protections for critical infrastructure was an important step forward, this morning's hearing demonstrated that there is much more work to be done to protect the networks that undergird the American economy.

One key area of vulnerability—the long supply chains for communications network equipment—is the subject of this afternoon's hearing. The globalization of the supply market for information and communications technology has undoubtedly created many benefits for our economy and coincided with incredible investment, competition, and innovation in the communications marketplace.

But it has also made it possible for our adversaries to exploit weaknesses during the design, production, delivery, and post-installation servicing of communications network equipment.

Industry and the federal government are working to respond to these threats.

As several of our witnesses this afternoon will discuss, companies are taking action to respond to supply chain risks. Voluntary industry consortia and public-private partnerships are also seeking to minimize these cyber exposures and I applaud these efforts.

But we should consider all options that could help minimize the cyber threats in the supply chain.

I look forward to hearing from GAO about its analysis of what other countries are doing in this area, as well as the potential benefits and drawbacks of adopting new review processes for purchases of foreign-manufactured communications equipment.

And I am pleased, Mr. Chairman, that the Subcommittee is convening a working group to examine supply chain security in more depth. The co-chairs of the working group—Representative Mike Rogers, who is the chairman of the House Intelligence Committee, and Representative Anna Eshoo, who has served on that committee, as well as the ranking member on this subcommittee—have great expertise from their service, as well as on both committees.

I look forward to our continued bipartisan work in this area. I thank all of the witnesses for being here and for their testimony. I want to apologize in advance that the conflict in schedule will keep me from being here to hear everything that is said, but I have staff listening in, I have got the testimony that I can review, and when the questions are asked and answered, I will be able to get a sense from those as well of the views that this very distinguished group will be giving to our subcommittee.

Thank you for this opportunity to give an opening statement. I thank all of you for being here today.

Mr. WALDEN. And the gentleman yields back the balance of his time. The good news is the votes now aren't going to come until 2:25 to 2:30, so we may actually get to hear from some of our witnesses.

And so we are going to start with Mr. Goldstein, who is the director of Physical Infrastructure Issues for the Government Accountability Office. Turn on your microphone, pull it close, and the next 5 minutes are yours, sir. Thank you for your work.

STATEMENTS OF MARK L. GOLDSTEIN, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; STEWART A. BAKER, PARTNER, STEPTOE AND JOHNSON, LLP, FORMER ASSISTANT SECRETARY FOR POLICY, DEPARTMENT OF HOMELAND SECURITY; JENNIFER BISCEGLIE, PRESIDENT AND CEO, INTEROS SOLUTIONS, INC.; ROBERT B. DIX, JR., VICE PRESIDENT, GOVERNMENT AFFAIRS AND CRITICAL INFRASTRUCTURE PROTECTION, JUNIPER NETWORKS, INC.; DAVID ROTHENSTEIN, SENIOR VICE PRESIDENT, GENERAL COUNSEL AND SECRETARY, CIENA; JOHN LINDQUIST, PRESIDENT AND CEO, ELECTRONIC WARFARE ASSOCIATES; AND DEAN GARFIELD, PRESIDENT AND CEO, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

STATEMENT OF MARK L. GOLDSTEIN

Mr. GOLDSTEIN. I will try not to take all of it.

Thank you, Mr. Chairman and members of the subcommittee. I am pleased to be here this afternoon to discuss issues surrounding the communications supply chain.

The United States is increasingly reliant on commercial communications networks for matters of national and economic security. These networks, which are primarily owned by the private sector, are highly dependent on equipment manufacturers in foreign countries. Certain entities in the Federal Government view this dependence as an emerging threat that introduces risks to the networks. GAO has requested review actions taken to respond to security risks from foreign manufactured equipment.

This testimony addresses how network providers and equipment manufacturers help ensure the security of foreign manufactured equipment used in commercial communications networks, how the Federal Government is addressing the risks of such equipment, and other approaches for addressing those risks and issues related to these approaches.

My testimony today is the public version of a national security sensitive report that GAO issued in May 2013. Information that the Department of Defense deemed sensitive has been omitted.

Let me briefly discuss the findings of the report that I may talk about today. First, the network providers and equipment manufacturers GAO spoke with reported taking steps in their security plans and procurement processes to ensure the integrity of parts and equipment obtained from foreign sources. Although these companies do not consider foreign manufactured equipment to be their most pressing security threat, their brand image and profitability depend on providing secure, reliable service.

In the absence of industry or government standards on the use of this equipment, companies have adopted a range of voluntary risk management practices. These practices span the lifecycle of equipment and cover areas such as selecting vendors, establishing vendor security requirements, and testing and monitoring equipment. Equipment that is considered critical to the functioning of the network is likely to be subject to more stringent security requirements according to these companies.

In addition to these efforts, companies are collaborating on the development of industry security standards and best practices and participating in information-sharing efforts within industry and with the Federal Government.

Second, the Federal Government has begun efforts to address the security of the supply chain for commercial networks. In 2013 the President issued an Executive Order to create a framework to reduce cyber risks to critical infrastructure, the National Institutes of Standards and Technologies, responsible for leading this effort, which is to provide technology-neutral guidance to critical infrastructure owners and operators.

NIST published a request for information, which it is conducting using a comprehensive review to obtain stakeholder input and develop the framework. You heard testimony on this effort this morning. NIST officials said the extent to which supply chain security of commercial communication networks will be incorporated into the framework is dependant in part on the input that they receive from stakeholders.

The Department of Defense considered the other federal efforts GAO identified to be sensitive to national security, and I cannot talk about them in a public forum.

And third, there are a variety of other approaches for addressing potential risks posed by foreign manufactured equipment and commercial communications networks. For example, the Australian government is considering a proposal to establish a risk-based regulatory framework that requires network providers to be able to demonstrate competent supervision and effective controls over their networks. The government would also have the authority to use enforcement measures to address noncompliance.

In the United Kingdom, the government requires network and service providers to manage risks and network security and can impose financial penalties for security breaches.

While these approaches are intended to improve supply chain security of communications networks, they may also create the potential for trade barriers and additional costs which the Federal Government would have to take into account if it chose to pursue such efforts.

Mr. Chairman, this concludes my oral statement. I would be happy to respond to comments. Thank you.

[The prepared statement of Mr. Goldstein follows:]

United States Government Accountability

GAO

Testimony

Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 2:00 p.m.
EDT
Tuesday, May 21, 2013

TELECOMMUNICATIONS NETWORKS

Addressing Potential Security Risks of Foreign-Manufactured Equipment

Statement of Mark L. Goldstein, Director
Physical Infrastructure Issues

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on federal and industry efforts related to communications supply chain security. The United States, like many other nations, is reliant on commercial communications networks for business and personal communication as well as for matters of national and economic security. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year. Many communications-based applications and services, including local and long-distance telephone calls, email, text messages, file transfers, and on-demand video programming, depend on effectively operating communications networks. Government, industry, and the public rely on communications networks to such a great degree that federal policy has included them in a category of national assets deemed critical infrastructure,[1] making their protection a national priority.[2] Many other critical infrastructure sectors such as banking and finance, energy, transportation systems, and water also rely

[1] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 1016(e), 115 Stat. 272, 401 (2001), codified at 42 U.S.C. § 5195c(e), defines critical infrastructure as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters," which is incorporated by reference by section 2(4) of the Homeland Security Act of 2002, Pub. L. No. 107-296, § 2(4), 116 Stat 2135, 2140 (2002), codified at 6 U.S.C. § 101(4).

[2] The White House, *Presidential Decision Directive/NSC 63* (Washington, D.C.: May 1998). The White House, *Homeland Security Presidential Directive 7* (Washington, D.C.: December 2003).

on communications networks to sustain their operation.[3] In addition, we have identified protecting systems that support our nation's cyber critical infrastructure as a government-wide high-risk area.[4]

U.S. communications networks are, by and large, owned, operated, and safeguarded by the private sector. Network providers are dependent on a global supply chain[5] to provide equipment—such as routers, switches, and elements of evolved packet cores[6]—that is used to transport a high volume of aggregated voice and data traffic over their commercial communications networks. According to several network providers, very little of this equipment is manufactured in the United States. Equipment manufacturers—including those headquartered in the United States—are heavily dependent on facilities in foreign countries to design, manufacture, and assemble their products. This dependence on foreign-

[3] Federal policy established 18 critical infrastructure sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; public health and health care; transportation systems; and water. Homeland Security Presidential Directive 7 identified 17 critical infrastructure sectors, and the Department of Homeland Security (DHS) added critical manufacturing using authority provided under the directive. The White House, *Homeland Security Presidential Directive 7* (Washington, D.C.: December 2003) and Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency* (2009).

[4] GAO's biennial high-risk list identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a government-wide high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure—referred to as cyber-critical infrastructure protection, or cyber CIP. See, most recently, GAO, *High-Risk* Series: An Update, GAO-13-283 (Washington, D.C.: February 2013).

[5] The National Institute of Standards and Technology (NIST) has defined the term "supply chain" to mean a linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of information and communications technology (ICT) products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer. *Notional Supply Chain Risk Management Practices for Federal Information Systems (October 2012) at* http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf.

[6] The evolved packet core is the core network used for long-term evolution (LTE) systems; a standard for commercial wireless technologies. LTE is widely accepted as the foundation for future mobile communications.

manufactured equipment[7] is viewed by some federal entities as an emerging threat that introduces potential risks[8] to the networks.[9] According to the Office of the National Counterintelligence Executive, "the globalization of the economy has placed critical links in the manufacturing supply chain under the direct control of U.S. adversaries."[10] A potential enemy or criminal group has a number of ways to potentially exploit vulnerabilities in the communications equipment supply chain, such as placing malicious code in the components that could compromise the security and resilience of the networks.[11]

Recent government efforts in the United States and other countries highlight concerns about the potential impact of supply chain threats on government, industry, and personal communications and transactions. Legislative proposals in the United States have sought to improve the protection of critical infrastructure, such as commercial communications

[7] For the purpose of this report, we define foreign-manufactured equipment as equipment produced, either in whole or in part, outside of the United States.

[8] NIST defines "threat" as any circumstance or event with the potential to adversely affect organizational operations and assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, or denial or disruption of service. According to NIST, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs, and (2) the likelihood of occurrence, which is based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability. NIST also defines "vulnerability" as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat. Department of Commerce, National Institute of Standards and Technology, *Glossary of Key Information Security Terms* (Washington D.C.: 2011).

[9] White House Cyberspace Policy Review, *Assuring a Trusted and Resilient Information and Communications Structure*. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[10] Office of the National Counterintelligence Executive, *Supply Chain Threats*, accessed on January 28, 2013, http://www.ncix.gov/issues/supplychain/index.php.

[11] Supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. We are not addressing disruptions that can be caused by labor or political disputes and natural causes (e.g., earthquakes, fires, floods, or hurricanes) that could affect the availability of equipment that is used to support the communication networks.

networks, from cyber attacks.[12],[13] Likewise, the White House released an Executive Order and a presidential policy directive in February 2013 that seek to improve the protection of critical infrastructure, including communications networks, from cyber attacks.[14] In 2012, the House Committee on Energy and Commerce, Subcommittees on Oversight and Investigations, and Communications and Technology held a series of hearings that addressed, among other things, cybersecurity[15] threats to communication networks.[16] The House Permanent Select Committee on Intelligence released a report in October 2012 in which it recommended the United States view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.[17] To help protect against the potential national security risks, the committee further recommended that U.S.-based network providers

[12] NIST defines "cyber attack" as an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information.

[13] Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013); the Cybersecurity and American Cyber Competitiveness Act, S. 21, 113th Cong. (2013).

[14] *Improving Critical Infrastructure Cybersecurity*, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (February 12, 2013). *Directive on Critical Infrastructure Security and Resilience,* Presidential Policy Directive 21, 2013 Daily Comp. Pres. Docs. No. 92. (February 12, 2013).

[15] According to NIST, "cybersecurity" means the ability to protect or defend the use of "cyberspace" from cyber attacks. NIST defines "cyberspace" as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

[16] House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, hearing on *IT Supply Chain Security: Review of Government and Industry Efforts* (Mar. 27, 2012). House Committee on Energy and Commerce, Subcommittee on Communications and Technology, hearings on *Cybersecurity and the Pivotal Role of Communications Networks*, March 7, 2012; and *Cybersecurity: Threats to Communications Networks and Public-Sector Responses*, March 28, 2012.

[17] Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, (Washington, D.C.: Oct. 8, 2012). The report states that the Chinese government or intelligence services could access equipment during the production process to insert malicious hardware or software for economic or foreign espionage with or without the cooperation of the companies. The report contains a classified annex that provides more information regarding the Committee's concerns about the risk. We did not access the annex.

consider the long-term security risks associated with purchasing products or services from specific foreign-based equipment manufacturers. Other countries—such as Australia, India, and the United Kingdom—are similarly concerned about the emerging threats to their commercial communication networks posed by the global supply chain and have taken actions to improve their ability to address this security challenge.

You asked us to examine private-sector and government actions to respond to the potential security risks posed by the use of foreign-manufactured equipment. This testimony is a public version of a sensitive report that we issued in May 2013 in response to your request. This testimony communicates the publicly releasable aspects of our findings while omitting information considered sensitive regarding federal actions taken to address potential security risks from foreign-manufactured equipment. This testimony discusses the objectives of our report, which were to examine:

1) How communications network providers and equipment manufacturers help ensure the security of foreign-manufactured equipment used in commercial communications networks.

2) How the federal government is addressing the potential risks of the use of foreign-manufactured equipment in commercial communications networks.

3) Other approaches for addressing the potential risks of the use of foreign-manufactured equipment in commercial communications networks and issues related to these approaches.

In preparing this statement, we relied on the work supporting our May 2013 report. For that report, we interviewed and collected documentation from federal agencies, including the Department of Commerce (Commerce), the Department of Homeland Security (DHS), the Department of Defense (DOD), the General Services Administration (GSA), and the Federal Communications Commission (FCC), among others, that have a role in addressing cybersecurity to identify federal efforts to address the risks of using foreign-manufactured equipment in commercial communications networks. We also asked federal agencies to identify statutes and regulations related to the federal government's legal and regulatory authority over how communications network providers ensure the security of their U.S. commercial networks.[18] We interviewed commercial communications network providers and equipment manufacturers that supply providers with routers, switches, and evolved packet cores to discuss their approaches for ensuring the security of the equipment used in commercial communications networks. We focused this work on the five wireless and five wireline network providers with the highest revenue and the eight manufacturers of routers and switches with the largest market share[19] in the United States. We did not test the effectiveness of the practices identified by the federal government, communication network providers, or equipment manufacturers.

Additionally, through a review of government and academic studies and interviews with stakeholders, we identified and described other approaches from governmental entities in Australia, India, and the United Kingdom that address supply chain risks for commercial communications networks.[20] We chose these countries to show the variation in how foreign governments are approaching supply chain risk management and because of the availability of public information in English describing their approaches. While the results of the data collected from these three countries may not encompass all possible approaches, they provided important insights into the approaches that some countries are using to address supply chain risks for commercial communications networks. We also assessed the potential for using the Committee on Foreign Investment in the United States (CFIUS)[21] review process for purchases of foreign-manufactured equipment. A voluntary notification process similar to CFIUS is being discussed by government and industry

[18] This report focuses on the wireline, wireless, and cable networks, and the core routing and switching equipment within those networks because they represent the majority of traffic.

[19] The eight manufacturers of routers and switches had a combined market share of 92 percent. We did not have access to data on market share for wireline and wireless providers.

[20] We attempted to include Canada in our review, but there was limited public information on its approach, and Canadian officials did not respond to our request for an interview.

[21] CFIUS is an inter-agency committee, established by Exec. Order No. 11858, 40 Fed. Reg. 20,263 (1975), as amended, authorized to review transactions that could result in control of a U.S. business by a foreign person, in order to determine the effect of such transactions on the national security of the United States.

stakeholders. We reviewed the Foreign Investment and National Security Act of 2007,[22] related regulations, and CFIUS annual reports to Congress to describe the CFIUS process and its applicability to purchases of foreign equipment for commercial networks. Finally, we conducted our own analysis regarding several potential issues that could arise from the use of these approaches. We identified these issues based on interviews with foreign government officials and U.S. industry stakeholders, and our review of foreign proposals and other documentation. The issues identified do not present an exhaustive list of all issues that could arise, but rather provide a range of considerations involved in other approaches to addressing supply chain risks.

We conducted this work from December 2011 to May 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for more information about our scope and methodology.

Background

Cybersecurity and Critical Infrastructure Protection Responsibilities

Federal policy calls for critical infrastructure protection activities that are intended to enhance the cyber and physical security of private infrastructures, such as telecommunication networks, that are essential to national and economic security. DHS, Commerce, and FCC have critical infrastructure protection responsibilities over issues related to the security of communications networks.[23] Appendix IV provides additional

[22] Pub. L. No. 110–49, 121 Stat. 246 (2007). *See,* also, 50 App. U.S.C. § 2061 note.

[23] Federal agencies can impose conditions on companies with which they contract. Network service providers and equipment manufacturers therefore may be subject to security requirements that are specific to contracts they have with the federal government. GSA officials told us that the Office of Management and Budget requires GSA to include supply-chain risk-management language in some of its critical-infrastructure-related contracts. The language requires documentation of a product's manufacturing chain of custody. However, according to GSA officials, this language is limited to critical-infrastructure-related contracts because of the higher cost of meeting the requirements.

information on these agencies' legal authority related to supply chain security for commercial communication networks. In addition, some executive actions have focused on supply chain risk management issues related to cybersecurity, which are described below.

Department of Homeland Security

The Homeland Security Act of 2002[24] established DHS and assigned it the following critical infrastructure protection responsibilities:

- develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States and
- disseminate, as appropriate, information to assist in the deterrence, prevention, and pre-emption of or response to terrorist attacks.[25]

Department of Commerce

Commerce is responsible under Presidential Policy Directive 21 (PPD-21), in coordination with other federal and nonfederal entities, for improving security for technology and tools related to cyber-based systems, and promoting the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.[26] Within Commerce, the National Institute of Standards and Technology (NIST) has responsibility for, among other things, cooperating with other federal agencies, industry, and other private organizations in establishing standard practices, codes, specifications, and voluntary consensus standards.[27]

Federal Communications Commission

Under PPD-21, FCC is responsible for exercising its authority and expertise to partner with other federal agencies on:

- identifying and prioritizing communications infrastructure;
- identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and

[24] 6 U.S.C. ch. 1.

[25] Homeland Security Act, § 201, 6 U.S.C. § 121(d)(5), (8).

[26] The White House, *Presidential Policy Directive 21* (Washington, D.C.: February 2013). Prior to PPD-21, Commerce was responsible under Homeland Security Presidential Directive 7, in coordination with other federal and nonfederal entities, for improving technology for cyber systems and promoting critical infrastructure efforts. The White House, Homeland Security Presidential Directive 7 (Washington, D.C.: December 2003).

[27] 15 U.S.C § 272.

- working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of the nation's critical communications infrastructure.[28]

Executive Actions

Supply chain risk management has been the focus of executive actions; for example, in January 2008, the President directed the development of a multi-pronged approach for addressing global supply chain risk management as part of the Comprehensive National Cybersecurity Initiative (CNCI), an ongoing effort.[29] More recently, at the direction of the President, a report on the federal government's cybersecurity-related activities was released, which discussed, among other things, the importance of prevention and response against threats to the supply chains used to build and maintain the nation's infrastructure.[30] Additionally, in response to one of the report's recommendations, the President appointed a national cybersecurity coordinator in December 2009.

Description of Core Networks and Access Networks

The United States has several nationwide voice and data networks that along with comparable communications networks in other countries, enable people around the world to connect to each other, access information instantly, and communicate from remote areas. These networks consist of core networks,[31] which transport a high volume of aggregated voice and data traffic over significant distances, and access networks, which are more localized and connect end users to the core network or directly to each other. Multiple network providers in the United

[28] The White House, *Presidential Policy Directive 21* (Washington, D.C.: February 2013).

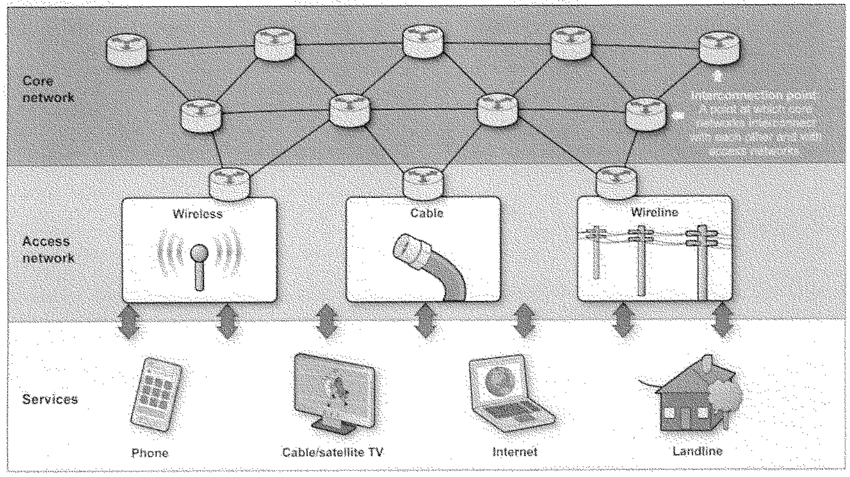
[29] The White House, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23.* (Washington, D.C.: Jan. 8, 2008).

[30] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. May 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[31] NIST officials stated that there are no agreed-upon definitions of "core network," "core equipment," or "core infrastructure." The descriptions of the terms in this report are based on information in the *2012 Risk Assessment Report for Communications*, published by DHS's National Communications System.

States operate distinct core and access networks that interconnect to form a national communications infrastructure (see fig. 1).

Figure 1: Communications Core and Access Networks



Sources: DHS and GAO.

Note: As stated previously, this testimony discusses only the wireline, wireless, and cable access segments of the communications sector.

Routers and switches send traffic, in the form of data packets, through core and access networks. These pieces of equipment read the address information located in the data packet, determine its destination, and direct it through the network. Routers connect users between networks, while switches connect users within a network.[32] The evolved packet core is the mobile core network used for long-term evolution (LTE) systems, a

[32] Many switches are now designed to perform the functions of routers as well as other security services such as firewalls and intrusion detection.

standard for commercial wireless technologies. LTE is widely accepted as the foundation for future mobile communications. Several major network equipment manufacturers are competing to provide equipment to wireless network providers that are upgrading their networks to deploy LTE.

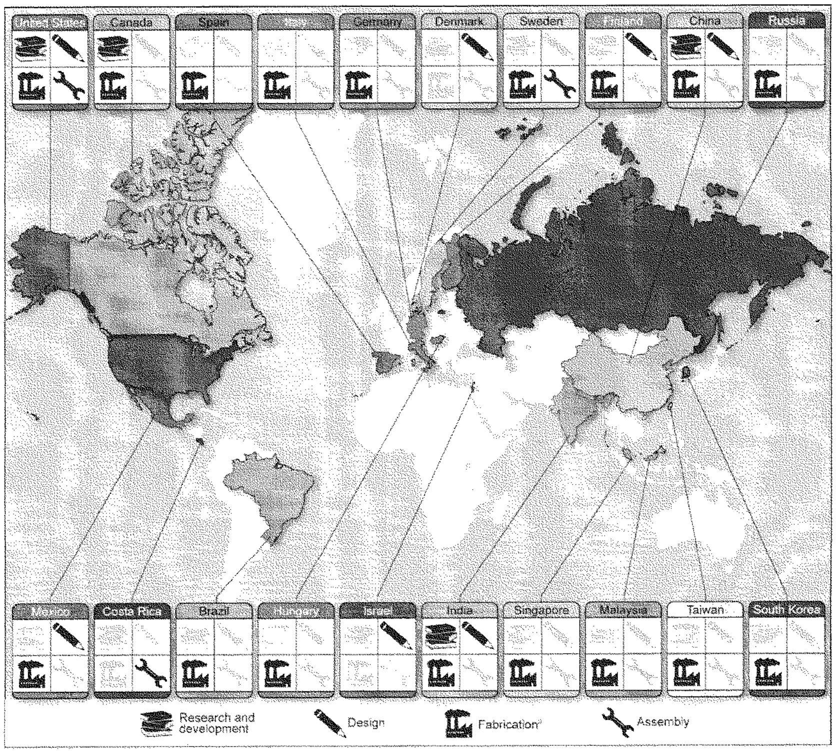
Global Supply Chain

Communications infrastructure is increasingly composed of components that are designed, developed, and manufactured by foreign companies or by U.S. companies that rely on suppliers that integrate foreign components into their products.[33] Furthermore, we have previously reported that according to NIST, today's complex global economy and manufacturing practices make corporate ownership and control more ambiguous when assessing supply chain vulnerabilities, as companies may conduct business under different names in multiple countries.[34] For example, foreign-based companies sometimes manufacture and assemble products and components in the United States, and U.S.-based companies sometimes manufacture products and components overseas or employ foreign workers domestically. Figure 2 depicts some of the locations that major network equipment manufacturers we spoke with use for different steps in the production process.

[33] Telcordia, *Mitigating the Supply Chain Security Risks in National Public Telecommunications Infrastructure,(* 2011).

[34] GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: March 23, 2012).

Figure 2: Examples of Supply Chain Locations for Network Equipment Manufacturers



Sources: GAO interviews with U.S. and non-U.S.-based equipment manufacturers and Map Resources.

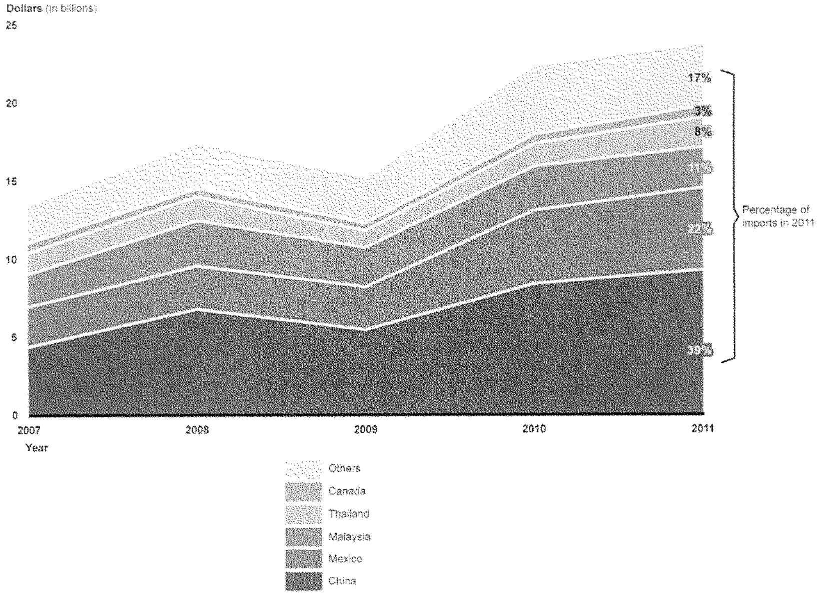
Note: Bold icons indicate that the production step is conducted in the country.

[a] Fabrication is the construction of a physical item from raw materials or the lowest-level parts.

From 2007 through 2011, communications network equipment imported for the U.S. market came from over 100 foreign countries.[35] While the import data do not distinguish whether the imports are from U.S. or foreign-based companies, according to International Trade Commission staff, many of the imports are from U.S. companies manufacturing abroad. Imports of network equipment to the United States grew about $10 billion (about 76 percent) over a 5-year period, from $13.5 billion in 2007 to $23.8 billion in 2011, as shown in figure 3. During this same period, imports from China, which was the leading source country, grew by $4.9 billion (112 percent). In 2011, the top five sources of U.S. imports of networking equipment were China ($9.3 billion), Mexico ($5.2 billion), Malaysia ($2.6 billion), Thailand ($1.9 billion), and Canada ($713 million).

[35] U.S. International Trade Commission. *Interactive Tariff and Trade DataWeb* (accessed Dec. 5, 2012). [Data file]. http://dataweb.usitc.gov/.The data are based upon a search for Harmonized Tariff Schedule (HTS) Code 851762, which includes machines for the reception, conversion, and transmission or regeneration of voice, images, or other data, including switching and routing apparatus.

Figure 3: Total U.S. Imports of Network Equipment and Top Five Sources by Country, 2007 to 2011



Source: GAO analysis of U.S. International Trade Commission staff data.

Note: The data included imports that were characterized as Harmonized Tariff Schedule Code 851762, which includes machines for the reception, conversion, and transmission or regeneration of voice, images, or other data, including switching and routing apparatus.

While there is no comprehensive unclassified compilation of attacks to core networks that originated in the supply chain,[36] reliance on a global

[36] Network providers may be reluctant to publicly divulge this information because of business concerns. For those incidents publicly reported, it can be difficult to discern if the attack was targeted to core network equipment.

supply chain introduces some degree of risk. Risks include threats posed by actors such as foreign intelligence services or counterfeiters that may exploit vulnerabilities in the supply chain, thus compromising the availability, security, and resilience of the networks.[37] Multiple points in the supply chain may present vulnerabilities that threat actors could exploit. For example, a lack of adequate testing for software patches and updates could leave a communications network vulnerable to the insertion of code intended to allow unauthorized access to information on the network. Routers and switches can present points of vulnerability because they connect to the core network and are used to aggregate data, according to an FCC official with whom we spoke. For example if a threat actor gained control of a router, that actor could disrupt data traffic to and inside core networks. Supply chain threats and vulnerabilities are discussed in more depth in appendixes II and III, respectively.

Industry Is Addressing the Risks of Using Foreign-Manufactured Equipment

Companies Address Supply Chain Risk through Procurement and Testing Practices

The network providers and equipment manufacturers we met with told us they address the potential security risks of using foreign-manufactured equipment through voluntary risk management practices. Officials from the companies and industry groups that we spoke with said that they consider the level of risk to be affected not by where equipment and components are made, but how they are made, particularly the security procedures implemented by manufacturers. Many of these officials also said they were not aware of any intentional attacks originating in the supply chain, and some said that they consider the risk of this type of attack to be low. Officials from four industry groups and one research institution we spoke with told us that supply chain attacks are harder to carry out and require more resources than other modes of attacks, such

[37] Supply chain-related threat actors include corporate spies, corrupt government officials, cyber vandals, disgruntled employees, foreign military, government agents or spies, radical activists, purveyors of counterfeit goods, or criminals. GAO-12-361.

as malicious software uploaded to equipment through the Internet, and, therefore, are the less likely vehicle to be used by potential attackers.[38] Three network providers told us the most common anomalies found in equipment are caused by erroneous coding in the software, anomalies that are unintentional. Such anomalies could, however, lead to exploitable vulnerabilities, according to officials from a third-party testing firm.[39] Nonetheless, the companies we spoke with told us that security is a high priority because their brand image and profitability depends, in part, on avoiding any type of breach of security or disruption of service.

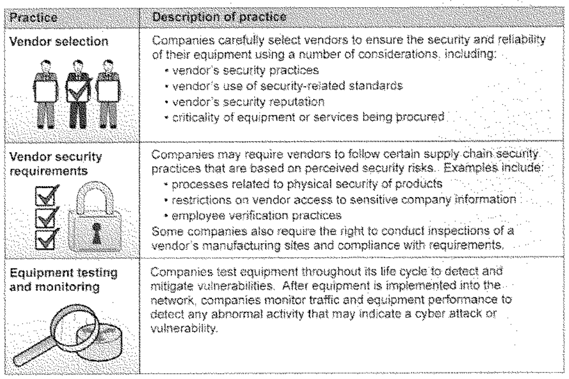
Network providers and equipment manufacturers told us that their voluntary risk management practices are in the areas of vendor selection, vendor security requirements, and equipment testing and monitoring, as described below and in figure 4. They said these practices are often a part of their company's overall security plans and procurement processes and are applied throughout the entire life cycle of their equipment.[40]

[38] Officials from an industry group and a research institution, as well as a recent congressional report also noted that a likely threat actor to carry out a supply chain attack would be a nation-state, because it may have the capabilities and the incentives for conducting such attacks.

[39] According to a recent congressional report and an official from a research institution that we spoke with, sophisticated implants in equipment, such as inserting malicious code into firmware, along the supply chain may be very difficult to detect. Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, (Washington, D.C.: Oct. 8, 2012).

[40] We did not test the effectiveness of these practices and have not described all the supply-chain risk-management practices that network providers and equipment manufacturers implement. Because we collected this information from the network providers and equipment manufacturers with the largest market shares, it may not be representative of the approaches taken by all companies.

Figure 4: Examples of Companies' Supply Chain Risk-Management Practices



Practice	Description of practice
Vendor selection	Companies carefully select vendors to ensure the security and reliability of their equipment using a number of considerations, including: • vendor's security practices • vendor's use of security-related standards • vendor's security reputation • criticality of equipment or services being procured
Vendor security requirements	Companies may require vendors to follow certain supply chain security practices that are based on perceived security risks. Examples include: • processes related to physical security of products • restrictions on vendor access to sensitive company information • employee verification practices Some companies also require the right to conduct inspections of a vendor's manufacturing sites and compliance with requirements.
Equipment testing and monitoring	Companies test equipment throughout its life cycle to detect and mitigate vulnerabilities. After equipment is implemented into the network, companies monitor traffic and equipment performance to detect any abnormal activity that may indicate a cyber attack or vulnerability.

Source: GAO.

Vendor Selection

The network providers and equipment manufacturers we spoke with said that ensuring the security and reliability of their equipment requires them to carefully select their vendors.[41] In addition to the typical considerations when selecting vendors—prices and product performance, the vendor's financial stability, and maintenance and service options offered—the providers and manufacturers told us that they consider security-related factors, such as the vendor's security practices, the industry standards related to security the vendors follow, and past security performance or reputation.[42] Another consideration for some network providers when selecting vendors is how critical the equipment being procured is to network operations. Components that will be used in the core network, for example, are typically purchased from vendors that network providers

[41] We refer to vendors in this section as those companies that supply network service providers with equipment or those that supply parts to equipment manufacturers.

[42] Network service providers and equipment manufacturers told us that there are quality-control and security-related industry standards for vendors that are not specific to supply chain, but do affect security, and a vendor's compliance with these maybe favorably viewed.

consider most trustworthy. Some network providers told us they also value having long-term relationships with equipment manufacturers, because they are able to develop trust over time that the manufacturer will provide them with reliable and secure equipment and services.

While network providers said that they are aware of security concerns about vendors from certain countries, they do not exclude vendors from consideration that have manufacturing locations in those countries, in part, because the global nature of the supply chain would make excluding all vendors located in a particular country difficult. Some network providers told us they may exclude or avoid vendors based on factors such as the ownership of the company or concerns about the security of the vendor's product, and two told us that federal government officials had advised against using specific vendors for national security reasons, as discussed in the following section of this testimony.

Vendor Security Requirements

Network providers and equipment manufacturers told us that once vendor selections are made, they might require vendors to follow certain security practices, often as part of their contracts. Network providers told us that the security practices they require are typically based on the criticality or perceived risk of the project and the role of the vendor. For example, one network provider we spoke with generates a vendor risk profile for purchases that it considers critical or high risk or if it does not have an established relationship with the vendor. The company uses the profile to collect information on the product or service being provided, the vendor's access to proprietary information, such as the company's financial information or customer sensitive information, and available information on a vendor's subcontractors. This information enables the network provider to identify areas of concern to investigate and to customize the security requirements placed on the vendor. The security practices that both network providers and equipment manufacturers may require of their vendors include the following:

- physical security measures, such as procedures for securing manufacturing sites, transporting equipment and parts, and packaging equipment and parts;
- access controls, such as limiting in-house and vendor employees' access to equipment, maintaining records of who accesses equipment, and restricting who performs patches and updates; and
- employee security measures, such as requiring employees to have background checks and use passwords and user verification to access systems.

Additionally, network providers and equipment manufacturers told us they might require vendors to allow inspections of their manufacturing sites to check for compliance with the agreed-upon security practices. Representatives from the companies we met with told us that they conduct inspections at varying frequencies and for a number of reasons, including if the vendor is providing a critical piece of equipment or part or is identified as high risk, or if the equipment is performing poorly.

Equipment Testing and Monitoring

Network providers and equipment manufacturers told us that equipment is tested to detect vulnerabilities. This is done throughout the life cycle of equipment, including during product development, before and after implementation, and when any patches or updates are applied. After equipment is installed into the network, network providers also monitor the equipment constantly to detect abnormal traffic or problems with the equipment that might indicate a potential cyber attack and disrupt network service. According to officials from a third-party testing firm, there are several tools available to test the security of equipment, including:

- *vulnerability scans*—searching software and hardware for known vulnerabilities;
- *penetration testing*—executing deliberate attempts to attack a network through the equipment, sometimes targeting specific vulnerabilities of concern; and
- *source code analysis*—evaluating in depth the underlying software code that can uncover unknown vulnerabilities that would not be detected during a vulnerability scan.[43]

Testing can be performed by the network provider, the equipment manufacturer, or independent third-party testing firms. Most network providers and several equipment manufacturers told us they use third-party testing firms on an ad-hoc basis, such as when requested by a customer or when they do not have the expertise or resources to conduct appropriate tests. Network providers and equipment manufacturers also use these firms when they want to analyze software or firmware source code because equipment manufacturers are reluctant to provide network

[43] There are other specialized tools available for certain situations. For example, officials from a third-party security firm told us that a network provider may conduct forensic analysis following a compromise of their network to provide a high level of assurance that the issue has been resolved.

providers with source code, which they consider intellectual property.[44] Two network providers and one equipment manufacturer told us they use a trusted delivery model that employs a third-party testing firm to ensure that the equipment purchased and received is secure. Under this model, the third-party testing firm tests equipment over the full life-cycle of equipment, including when there are software patches or hardware updates, and uses a number of different techniques, such as source code analysis. Additionally, the testing firm verifies that the equipment delivered and implemented by the network provider matches the equipment tested and that the equipment manufacturer followed certain security procedures.

However, a recent congressional report identified the following potential limitations of third-party testing and available testing techniques.

- These firms typically test equipment that is configured in a specific and restrictive way that may differ from the configuration that is actually deployed in the network.
- The behavior of equipment can vary widely depending on how and where it is configured, installed, and maintained.
- The pace of technology is changing more rapidly than third-party evaluation processes.
- Vendors that finance their own security evaluations create a conflict of interest that can lead to skepticism about the independence and rigor of the result.[45]

Officials from a third-party testing firm told us that there are evaluation processes, such as the trusted delivery model, that test the equipment delivered to network providers and deployed into the network against the equipment tested. Although they said it is impossible to test every piece of equipment, the firm tests a statistically significant random selection of equipment that represents all manufacturing lots and geographic

[44] Firmware is the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

[45] Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, (Washington, D.C.: Oct. 8, 2012).

locations. They also told us that independence is critical to their business. The officials said the vendor has no visibility into the evaluation process, and, typically, the vendor is obligated to report testing results.

The congressional report further stated that regardless of the testing technique employed, fully preventing a determined and clever insider from intentionally inserting flaws into equipment means finding and eliminating every significant vulnerability from a complex product, a monumental, or even—in the words of one congressional report—"virtually impossible" task.[46] Similarly, officials from one third-party testing firm whom we spoke with told us that they have concerns about the effectiveness of network monitoring as a way of detecting vulnerabilities. They said that security monitoring, in most cases, can only detect attempts to exploit known vulnerabilities, or in more complex approaches, identify potentially dangerous anomalous network activity. And as systems evolve and are updated, new vulnerabilities that have long existed in the underlying equipment may be inadvertently exposed in a manner that makes exploitation possible.

Companies Collaborate on Supply-Chain Security Standards, Best Practices, and Information Sharing

There are currently no industry standards that address all aspects of supply chain risk management, including supply chain security, and few best practices that provide industry with guidance on determining what practices to use. However, according to officials from companies and industry groups and the experts we spoke with, there are several industry-led efforts to establish standards and best practices and share information related to supply chain security.[47] Some network providers and equipment manufacturers told us that they developed their own practices based on national and international standards that address information systems' security, such as those practices described within

[46] Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, (Washington, D.C.: Oct. 8, 2012).

[47] Stakeholders we spoke with told us about efforts related to securing the software supply chain, such as those conducted by the Software Assurance Forum for Excellence in Code, which is an industry-led group that develops best practices for reliable software, hardware, and services and DHS's Software Assurance Program. These groups have published several supply-chain security guidelines for the development of secure software.

the certification program called the Common Criteria,[48] and those developed by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), NIST, and the Internet Engineering Task Force. However, these standards are not specific to supply chain security.[49] Additionally, federal agencies that we have identified as having jurisdiction over issues related to the security of communications networks have not established supply chain security requirements for the communications industry, as discussed further in the next section of this testimony.[50] The companies we spoke with also told us they have been participating in information sharing about cybersecurity issues, including supply chain security, in venues including informal conversations, industry group meetings, and discussions with the federal

[48] The Common Criteria provides a common set of requirements for the security functionality of information technology (IT) products and for assurance measures applied to these IT products during evaluation. Evaluations of IT products are conducted by independent and licensed laboratories, and those that meet the Common Criteria requirements are provided with a certification. These certifications are recognized by participating member countries.

[49] According to a DOD official, there are a number of national and global standards-development organizations—such as ISO, the Common Criteria's technical working group, and the Common Criteria Development Board—that have supply-chain risk-management-related initiatives. According to officials from NIST and DOD, one of the more significant standards being developed is ISO/IEC 27036 "IT Security—Security techniques—Information security for supplier relationships." This draft standard will offer guidance on the evaluation and mitigation of security risks involved in the procurement and use of information or IT-related services supplied by other organizations. NIST officials told us that the proposed standard would address the risk management aspects of the entire ICT supply chain from the perspectives of suppliers and customers. DOD officials told us that all of the supply-chain risk- management initiatives and standards development activities are monitored and harmonized where possible.

[50] In October 2012, NIST published an interagency report that describes a set of supply-chain assurance methods and practices to help federal departments and agencies manage the associated information and communications technology (ICT) supply-chain risks over the entire life cycle of ICT systems, products, and services. NIST officials told us that they are developing a special publication related to this report. Several network providers and equipment manufacturers we spoke with said that these could serve as a reference for private companies to use when developing their own supply-chain risk-management practices. *Notional Supply Chain Risk Management Practices for Federal Information Systems* (October 2012) at http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf.

government. Below are the two industry-led efforts most frequently discussed during our interviews.[51]

The Open Group Trusted Technology Forum (OTTF)

The OTTF is a forum within The Open Group, which is a global consortium that represents all sectors of the IT community including academics, equipment manufacturers, federal agencies, and software developers. The Open Group establishes certification programs and voluntary consensus standards, such as standards for security, enterprise architecture, interoperability, and systems management.[52] The OTTF's objective is to create and adopt standards to improve the security and integrity of commercial off-the-shelf information and communication products, including hardware and software, as they are being developed and moved through the global supply chain. In April 2013, the OTTF published a voluntary standard[53] that is intended to enhance the security of global supply chains by mitigating the risks of tainted and counterfeit products.[54] The OTTF intends to provide an accreditation program that will allow information and communication providers, equipment manufacturers, and those vendors that supply software or hardware components to the providers and manufacturers, to become accredited if they meet the standard's requirements and conformance criteria. Officials from DOD said that although it is unknown whether industry will adopt this standard and what the associated costs will be to maintain and use it, developing such process-based certifications along with product

[51] Academics and equipment manufacturers we spoke with also told us about a set of supply-chain-security best practices being developed by the Internet Security Alliance (ISA)—a multi-sector trade association whose mission is to motivate enhanced security of cyber systems. According to an ISA official, ISA has drafted a set of voluntary best practices that were developed through recommendations from industry and government. The document provides electronics manufacturers with a set of security measures for all stages of the production of electronics products that when implemented, will make it more difficult to insert malicious firmware or defective components into electronics products, such as limiting the personnel with access to design facilities to those who genuinely need to be there and using two or three factor authentication (e.g., photo radio-frequency identification and fingerprint) for employees.

[52] Officials from the Open Group told us their standards are consistent with the Office of Management and Budget Circular No. A-119, which establishes policies on federal use and development of voluntary consensus standards and conformity assessment activities.

[53] The Open Group, *Open Trusted Technology Provider Standard (O-TTPS)™ Version 1.0, Mitigating Maliciously Tainted and Counterfeit Products* (April 2013).

[54] Information and communication providers—including network providers and equipment manufacturers, government organizations, and third-party labs—participated in the OTTF's effort to establish this voluntary standard.

certifications, such as the Common Criteria, may prove beneficial in covering more of the global IT supply chain.[55]

Communications Sector Coordinating Council (CSCC)

In accordance with Homeland Security Presidential Directive 7, the CSCC is an industry-led group that represents the viewpoints from the U.S. communications sector and facilitates coordination between industry and the federal government on improving physical and cyber security of the communications critical infrastructure.[56],[57] Representatives from the CSCC told us that the CSCC began meeting with the federal government in March 2011 to discuss supply chain security, which led to the creation of a CSCC working group to facilitate dialogue, planning, and coordination among the government and industry on supply chain risk management. This group's objectives include enhancing the government's understanding of industry's current risk management practices, the government's sharing of supply chain threat information,

[55] The Permanent Select Committee on Intelligence report cited the earlier stated concern that evaluation programs, such as the Common Criteria, that rate companies based on their processes do not address the threats because the evaluation does not include testing for vulnerabilities in the equipment. This concern could apply to the OTTF's standard because it also is based on certifying vendors' processes and not on evaluations of the equipment's integrity.

[56] Federal policy established 18 critical infrastructure sectors that are critical to the nation's security, economy, and public health and safety. The National Infrastructure Protection Plan (NIPP) presents the government's coordinated approach that will be used to establish priorities, goals, and requirements for critical infrastructure and key resources protection. The plan specifies key initiatives, milestones, and metrics to achieve the Nation's critical infrastructure and key-resources-protection mission. The NIPP also describes a partnership model as the primary means of coordinating government and private sector efforts in this area. For each sector, the model requires formation of government coordinating councils and encourages the formation of sector coordinating councils. Sector coordinating councils are self-organized, self-run, and self-governed entities comprised of critical infrastructure owners and operators that serve as the principals for sector policy coordination and planning. DHS is the sector-specific agency assigned to the communications sector that according to the NIPP, is to work with its private sector counterparts to understand and mitigate cyber risk. Department of Homeland Security, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (2009).

[57] In February 2013, the White House released *Presidential Policy Directive 21* (PPD 21), which requires DHS to update the NIPP. PPD 21 specifically stated that the update to the NIPP "should consider sector dependencies on energy and communications systems." The White House, *Presidential Policy Directive 21* (Washington, D.C.: February 2013). According to DHS officials, following the release of the revised NIPP in late 2013, an updated communications sector-specific plan will be released, and it will address supply chain security of communications networks.

and identifying and sharing best practices for supply chain risk management. The working group is scheduled to conclude its work in December 2013.[58]

Federal Government Has Begun Efforts to Address the Risks of Using Foreign-Manufactured Equipment

The White House released an Executive Order in February 2013 that is likely to have an impact on communications supply chain security. We identified other federal efforts, such as the Interim Telecommunications Sector Risk Management Task Force, that could impact communications supply chain security, but the results of those efforts are considered sensitive, so we do not include them here.

Executive Order on Cybersecurity for Critical Infrastructure

An Executive Order released in February 2013 calls for NIST to develop a framework to reduce cyber risks to critical infrastructure and for DHS and others to spearhead increased information sharing between the federal government and owners and operators of critical infrastructure including communications networks.[59] As discussed below, federal officials told us that supply chain security may be included in these efforts, but the extent has yet to be determined.

Cybersecurity Framework

The Executive Order instructs NIST to develop a cybersecurity framework (framework) to reduce cyber risks to critical infrastructure using an open public review and comment process. This framework would provide technology-neutral guidance to critical infrastructure's owners and operators. In February 2013, NIST published a request for information (RFI) in which NIST stated it is conducting a comprehensive review to

[58] While the working group is currently set to end in December 2013, it may be extended beyond that date if necessary. According to one member, the working group had met twice as of December 2012.

[59] Exec. Order No. 13,636. As previously mentioned, the Executive Order seeks to improve the protection of critical infrastructure.

develop the framework and is seeking stakeholder input.[60] According to NIST officials, the extent to which supply chain security of commercial communications networks will be incorporated into the framework is largely dependent on the input it receives from stakeholders. The officials added that while it is reasonable to assume that they may receive comments about supply chain security, which crosses critical infrastructure sectors, it is possible they may not receive comments specific to the use of foreign-manufactured equipment in commercial communication networks.

In adopting the preliminary framework, the Executive Order requires agencies with responsibility for regulating the security of critical infrastructure[61] to provide a report—in consultation with national security staff, DHS, and the Office of Management and Budget—which states whether the agencies have clear authority to establish requirements based on the framework and whether any additional authorities are necessary. DHS officials stated that without seeing the context of the report, they could not say whether it would identify authorities specifically related to the supply chain security of commercial communications networks and the conditions under which those authorities could be used.

Information Sharing

The Executive Order also calls for the federal government to increase information sharing with owners and operators of critical infrastructure, including communications networks, information sharing that could

[60] National Institute of Standards and Technology. *Developing a Framework To Improve Critical Infrastructure Cybersecurity* (February 2013), accessed March 4, 2013, https://federalregister.gov/a/2013-04413. The RFI seeks comments on several topics including current risk management practices; use of frameworks, standards, guidelines, and best practices; the applicability of existing publications, including those of other governments; and specific industry practices. NIST has invited responses from owners and operators of critical infrastructure; federal agencies; state and local governments; standard-setting organizations; and other stakeholders.

[61] FCC, to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies on (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices. The White House, *Presidential Policy Directive 21* (Washington, D.C.: February 2013).

include sharing of supply chain-related threats.[62] The order directs DHS to share unclassified cyber threat information and expand a voluntary information-sharing program that provides classified cyber threat information to critical infrastructure owners and operators with government security clearances. DHS officials told us that they foresee that this information sharing could encompass threats originating in the supply chain.

Other Approaches to Supply Chain Risk Management

Risk Management Approaches from Selected Countries

Australian Reform Proposal

The Australian government is considering a reform proposal to establish a risk-based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure.[63] The Attorney-General, in consultation with industry, has created a proposal that addresses supply chain risks by introducing a universal obligation on

[62] Federal agencies have multiple cyber-threat information-sharing mechanisms in partnership with the private sector, though these do not always address supply chain concerns. The mechanisms include the National Coordinating Center/Communications Sector Information Sharing and Analysis Center, Network Security Information Exchange, the National Security Telecommunications Advisory Committee, Cybersecurity Information Sharing and Collaboration Program, National Infrastructure Coordinating Center, and the United States Computer Emergency Readiness Team.

[63] For the purposes of security, Australia's telecommunication industry is regulated primarily under two pieces of legislation—the Australian Telecommunications Act (1997) administered by the Minister for Broadband, Communications and the Digital Economy and the Australian Telecommunications (Interception and Access) Act (1979) (TIA Act), administered by the Attorney-General. The TIA Act does not specifically address supply chain risks, hardware and software vulnerabilities or security risks to the confidentiality, integrity and availability of telecommunications infrastructure. See Australian Government, Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats* (July 2012).

carriers and carriage service providers[64] to protect their networks and facilities from unauthorized access or interference. Specifically, the proposal requires carriers and carriage service providers to be able to demonstrate competent supervision and effective controls over their networks. The government would also have the authority to use enforcement measures to address noncompliance, as described in table 1.[65]

Table 1: Key Security Requirements of Australia's 2012 Reform Proposal

Key security requirements	Description
Competent supervision	Carriers and carriage service providers would be required to maintain 1) oversight (either in-house or through a trusted third party) of their network operations and the location of data; 2) awareness of, and authority over, parties with access to network infrastructure; and 3) a reasonable ability to detect security breaches or compromises.
Effective control	Carriers and carriage service providers would be required to maintain direct authority or contractual arrangements which ensure that their infrastructure and the information held on it are protected from unauthorized access. This could include arrangements to terminate contracts for security breaches and remove information and network systems where unauthorized access to a network has occurred.
Demonstration of compliance	Carriers and carriage service providers would be required to demonstrate compliance through steps such as compliance assessments and audits.
Enforcement measures/penalties for noncompliance	Government enforcement options include the authority to direct carriers and carriage service providers to undertake targeted mitigation of security risks, including modifications to infrastructure, audits, and ongoing monitoring, with costs covered by the carriers and carriage service providers; and financial penalties. The Attorney-General would also retain the power to order carriers and carriage service providers to stop service for the most serious security breaches.

Source: GAO analysis of Australian reform proposal.

Under this framework, the government would provide guidance to inform carriers and carriage service providers how they can maintain competent supervision and effective control over their networks and educate carriers and carriage service providers on national security risks. The approach

[64] Australia defines a "carrier" as an owner of a telecommunications facility that is used to supply carriage services to the public. It defines a "carriage service provider" as an entity that supplies a carriage service to the public using a telecommunications facility.

[65] See Australian Government, Attorney-General's Department, *Equipping Australia against Emerging and Evolving Threats* (July 2012).

would require amendments to telecommunications statutes, such as the Telecommunications Act and other relevant laws.[66]

India's Licensing Amendments

India enacted a new approach in 2011 through its operating licenses for telecommunications service providers.[67] India's Department of Telecommunications (DoT) is responsible for granting operating licenses to India's telecommunications service providers. In May 2011, DoT issued amendments to its operating licenses that included new or revised requirements for providers and equipment vendors to improve the security of India's telecommunications network infrastructure.[68] Under the amendments, telecommunications service providers are to be completely responsible for security of their networks, including the supply chain of their hardware and software. Key security requirements are described in table 2.

Table 2: Key Security Requirements of India's 2011 Licensing Amendments

Key security requirements	Description
Organizational security policies	Providers must have an organizational policy on security and security management of their networks and must audit their own networks or contract with a network-security audit and certification agency to provide a network audit at least once a year.

[66] Australian Government, Attorney-General's Department, *Equipping Australia against Emerging and Evolving Threats* (July 2012).

[67] In addition to the licensing approach, in February 2012, India also adopted a Preferential Market Access designed, in part, to address unspecified security concerns of the Indian government. The policy provides preference to electronic products manufactured in India in government procurements. According to the Office of the United States Trade Representative (USTR), the policy also anticipates requiring private firms to ensure that their purchases of "electronic products which have security implications" are domestically manufactured. USTR officials told us the federal government and industry, joined by other governments and foreign industry associations have raised concerns with the government of India regarding the scope and substance of this approach.

[68] Government of India, Department of Telecommunications, Letter to All Unified Access Service Licensees, No. 10- 15/2011-AS.III/(21), (May 31, 2011) (amending license clause 41.6A). USTR and others have reported that India's previous amendments to telecommunications service licenses included several controversial requirements for foreign vendors, including the forced transfer of technology to Indian companies, the escrowing of source code and other high-level and detailed designs, and assurances against malware and spyware during the entire use of the equipment. According to USTR, in response to concerns raised by industry and trading partners, including the United States, India suspended implementation of the license amendments while it consulted interested parties to better evaluate the extent to which those requirements in fact addressed India's security challenges.

Key security requirements	Description
Local testing requirements	Beginning April 1, 2013, all network equipment must be tested and certified to relevant Indian or international security standards in Indian labs.
Recordkeeping	Telecommunications service providers must keep a record of the supply chain of their hardware and software.
Inspection provisions	Vendors must permit the providers, DoT, or its designee to inspect the hardware, software, design, development, manufacturing facility and supply chain and subject all software to a security/threat check at any time.
Enforcement measures/penalties	DoT can issue financial penalties for inadvertent security breaches or acts of intentional omissions, such as a deliberate vulnerability left in equipment. In addition, DoT may cancel the license of the provider and blacklist the vendor that supplied the hardware or software that caused the security breach.

Source: GAO analysis of India's May 2011 Licensing Amendments.

United Kingdom's Security Requirements and Cybersecurity Evaluation Centre

The United Kingdom (UK) enacted new security and resilience requirements for network and service providers in 2011 through revisions to its Communications Act of 2003.[69] The UK's Office of Communications (Ofcom), the independent regulator and competition authority for the UK communications industries, is responsible for enforcing the requirements. According to Ofcom officials, these requirements address supply chain risks by focusing on the ability of the network and service providers to manage the overall security of their infrastructure and maintain network availability. Ofcom officials told us they are still developing their overall approach to enforcing the requirements, which are described in table 3.

Table 3: Key Security Requirements for UK Network and Service Providers Enacted in 2011

Key security requirements	Description
Risk management	Network and service providers must take appropriate measures to manage risks to the security of the networks including management of general security risks; protecting end users; protecting interconnections; and maintaining network availability.
Incident reporting	Network and service providers must notify Ofcom of security breaches or reductions in availability that have a significant impact on the network or service.
Demonstration of compliance	Providers must demonstrate that a basic range of security measures have been taken. This could include compliance with security standards, such as ISO 27000 and ND1643.[a]

[69] See Section 105A-D of the UK Communications Act of 2003. The UK government introduced the new security and resilience requirements, which were effective as of May 2011, to implement changes required by revisions to the regulatory framework set by the European Commission. This framework applies to all transmission networks and services used for electronic communications in European Member States. See, Ofcom, *Ofcom Guidance on Security Requirements in the Revised Communications Act 2003* (February 2012).

Key security requirements	Description
Enforcement measures/penalties	Ofcom could issue binding instruction to direct a provider on the steps that must be taken to improve the security of their network. For serious requirements breaches, Ofcom can impose financial penalties.

Source: GAO analysis of UK security requirements.

[a] ND 1643 is a minimum security standard for network interconnection developed by Network Interoperability Consultative Committee, a technical forum for the UK communications sector that develops interoperability standards for public communications networks and services in the UK.

A Chinese network equipment manufacturer voluntarily partnered with the UK government to establish a Cybersecurity Evaluation Centre to test its equipment for use in UK networks. According to officials from Ofcom and the Chinese manufacturer, the facility was created in part to address national security concerns related to using equipment from a vendor that did not have an established relationship with the UK government or UK network providers. The Chinese manufacturer provides the facility with the design and source code for all equipment, which is then tested for vulnerabilities by staff with UK security clearances. According to officials from Ofcom and representatives from the Chinese manufacturer, network providers cannot use the equipment until it has been approved through the testing process. In addition, the UK government requires all software patches be tested using the same process before they are installed on the equipment by the network providers. According to officials from the Chinese manufacturer, this voluntary approach helped increase trust with its customers. However, in November 2012, the chairman of the UK parliament's intelligence and security committee confirmed to us that the committee is reviewing the commercial relationship between the Chinese manufacturer and a British telecommunications provider and the Chinese manufacturer's overall presence in the UK's critical national infrastructure.[70]

[70] Representatives from the UK parliament's intelligence and security committee declined to provide additional details about the inquiry.

Expanding Use of the U.S. Process for Reviewing Foreign Acquisitions

The U.S. government's Committee on Foreign Investment in the United States (CFIUS) conducts reviews to determine whether certain transactions that could result in foreign control of U.S. businesses pose risks to U.S. national security.[71] Industry representatives from the U.S. Communications Sector Coordinating Council told us the council and participating federal entities are discussing whether a voluntary notification process similar to CFIUS should be used for network provider purchases of foreign-manufactured equipment. In addition, the House Intelligence Permanent Select Committee report recommended that legislative proposals seeking to expand CFIUS to include purchasing agreements should receive thorough consideration by relevant congressional committees.[72]

CFIUS follows a process established by statutes and regulations for examining certain transactions that could result in foreign control of U.S. businesses. Parties generally submit voluntary notices of transactions to CFIUS, but CFIUS also has the authority to initiate reviews unilaterally.[73] Pursuant to the Foreign Investment and National Security Act of 2007,[74] CFIUS must complete a review of a covered transaction[75] within 30

[71] The members of CFIUS include the heads of the Departments of Treasury, Justice, Homeland Security, Commerce, Defense, State, and Energy, and Offices of the U.S. Trade Representative and Science and Technology Policy. The following offices also observe and, as appropriate, participate in CFIUS's activities: Office of Management and Budget, Council of Economic Advisors, National Security Council, National Economic Council, and Homeland Security Council. The Director of National Intelligence and the Secretary of Labor are non-voting, ex-officio members of CFIUS with roles as defined by statute and regulation.

[72] Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Washington, D.C.: Oct. 8, 2012).

[73] 31 C.F.R. §§ 800.401 (procedures for notice), 800.402 (contents of voluntary notice), See also, Department of Treasury, "Committee on Foreign Investment in the United States Process Overview," accessed January 8, 2013, http://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-overview.aspx.

[74] Pub. L. 110–49, 121 Stat. 246 (2007), amending the Defense Production Act of 1950, § 721, Act of Sept. 8, 1950, ch. 932, 64 Stat. 798, codified at 50 App. U.S.C. § 2170.

[75] The term "covered transaction" means any merger, acquisition, or takeover that is proposed or pending after August 23, 1988, by or with any foreign person, which could result in control of a U.S. business by a foreign person. 50 App. U.S.C. § 2170(a)(3); 31 C.F.R. §§ 800.207 and 800.224 .

days.[76] In certain circumstances, following the review, CFIUS may initiate an investigation that may last up to 45 additional days.[77],[78] If CFIUS finds that the covered transaction presents national security risks and that other provisions of law do not provide adequate authority to address the risks, then CFIUS may enter into an agreement with, or impose conditions on, the parties to mitigate such risks. If the national security risks cannot be resolved and the parties do not choose to abandon the transaction, CFIUS may refer the case to the President, who can choose whether to suspend or prohibit the transaction.[79],[80] As shown in table 4, presidential decisions are rare. Table 4 also shows the number of CFIUS covered transactions, withdrawals, and other outcomes from calendar years 2009 to 2011.

[76] 50 App. U.S.C. § 2170(b)(1)(E); 31 C.F.R. § 800.502 (beginning of thirty-day review). *See also,* Department of Treasury, "Committee on Foreign Investment in the United States Process Overview," accessed January 8, 2013, http://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-overview.aspx.

[77] 31 C.F.R. §§ 800.503 (determination of whether to undertake an investigation), 800.504 (determination not to undertake an investigation), 800.505 (commencement of investigation), 800.506 (completion or termination of investigation and report to the President). See also, Department of Treasury, "Committee on Foreign Investment in the United States Process Overview," accessed January 8, 2013, http://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-overview.aspx.

[78] Parties to a transaction may request withdrawal of their notice at any time during the review or investigation stages. CFIUS must approve the requests and may include conditions on the parties, such as requirements that they keep CFIUS informed of the status of the transaction or that they re-file the transaction at a later time. *See* 31 C.F.R. § 800.507 (withdrawal of notice). CFIUS tracks withdrawn transactions. See Department of Treasury, "Committee on Foreign Investment in the United States Process Overview," accessed January 8, 2013, http://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-overview.aspx.

[79] See Department of Treasury, "Committee on Foreign Investment in the United States Process Overview," accessed January 8, 2013, http://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-overview.aspx.

[80] If CFIUS finds that the transaction in a notice does not present any national security risks or that other provisions of law provide adequate and appropriate authority to address the risks, then CFIUS will advise the parties in writing that CFIUS has concluded all action for the transaction.

Table 4: Committee on Foreign Investment in the U.S.'s Covered Transactions, Withdrawals, and Presidential Decisions, Calendar Years 2009 to 2011

Year	Number of covered transactions	Number of reviews concluded	Number of covered transactions withdrawn during review	Number of investigations concluded	Number of covered transactions withdrawn during investigations	Presidential decisions
2009	65	35	5	23	2	0
2010	93	52	6	29	6	0
2011	111	70	1	35	5	0
Total	**269**	**157**	**12**	**87**	**13**	**0**

Source: GAO analysis of Department of Treasury data.

Discussions between the Communications Sector Coordinating Council and participating federal entities on adapting a CFIUS-type voluntary notification process for use on equipment purchases are ongoing, and it is not clear how the proposal will develop, if at all.[81] The council is trying to understand the threats the government is concerned about and whether these could be best addressed by a CFIUS- type process or some other means. According to some members of the council, options range from a simple notification process, wherein network providers notify the federal government of proposed equipment purchases, to a complete review and approval process of the proposed transactions, including the aforementioned 30-day review and 45-day investigation periods.[82]

[81] Similarly, in its discussion paper describing its reform proposal, the Australian government noted that it initially proposed using a notification obligation for procurements in place of the requirement to provide information to the government on request. The Australian government also indicated that industry expressed a preference for an approach that avoids the need for government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it. See, Australian Government, Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats* (July 2012).

[82] As previously mentioned, the Interim Telecommunications Sector Risk Management Task Force is also considering a voluntary transactional review process, where network providers notify the government when they make equipment purchases or significant changes to their networks.

Potential Issues Related to Use of These Approaches

While these approaches are intended to improve supply chain security of communications networks,[83] they may also create the potential for trade barriers, additional costs, and constraints on competition. Additionally, there are other issues specific to the approach of expanding the CFIUS process to include foreign equipment purchases. We identified these issues based on interviews with foreign government officials and U.S. industry stakeholders, and our review of foreign proposals and other documentation. While the issues we identified provide a range of considerations that U.S. federal agencies would need to take into account if they chose to implement these approaches, they do not represent an exhaustive list.[84]

Trade Barriers and Disputes

Some of the approaches may create a trade barrier or cause trade disputes. The Office of the United States Trade Representative (USTR) has reported that standards-related measures that are non-transparent, discriminatory, or otherwise unwarranted can act as significant barriers to U.S. trade.[85] USTR has reported concerns regarding some of India's licensing requirements for telecommunications service providers including the following:

- the requirement for telecommunications equipment vendors to test all equipment in labs in India;
- the requirement to allow the service provider and government agencies to inspect a vendor's manufacturing facilities and supply chain and perform security checks for the duration of the contract to supply the equipment; and
- the imposition of strict liability and possible blacklisting of a vendor for taking inadequate precautionary security measures, without the right to appeal and other due process guarantees.[86]

[83] This is not an exhaustive list of all approaches. See appendix I for more detail on selection criteria.

[84] See appendix I for more detail on selection criteria for the factors.

[85] Office of the United States Trade Representative, *2011 Report on Technical Barriers to Trade* (Washington, D.C.: 2012).

[86] Office of the United States Trade Representative, *2012 Section 1377 Review On Compliance with Telecommunications Trade Agreement,* (Washington, D.C.: 2012). USTR officials and other industry stakeholders are working with the Indian government to help ensure that U.S. can participate in the Indian market, while respecting the security concerns of its government.

These requirements may result in trade-distorting conditions by making it more expensive and burdensome for foreign equipment manufacturers to do business in India. According to USTR, it is too early to evaluate whether the proposed reforms in Australia, new requirements and voluntary Cybersecurity Evaluation Centre in the UK, and an extension of CFIUS to equipment purchases would create trade barriers or cause trade disputes. Three U.S.-based equipment manufacturers told us that extending CFIUS to equipment purchases could cause other countries to implement similar policies, which may result in barriers to entry in other countries and trade disputes.[87]

Costs

All of the approaches may increase costs to industry and the federal government. The Australian and UK governments recognize that changes to the regulatory framework would include a cost to industry, which may increase prices for consumers.[88] Representatives from the Chinese equipment manufacturer stated that although voluntarily setting up the Cybersecurity Evaluation Centre was expensive, it was the cost of doing business in the UK. Similarly, one telecommunications industry group reported that India's 2011 License Amendments would increase compliance costs for Indian telecommunications services providers.[89] The majority (6 of 8) of equipment manufacturers we spoke with told us that any proposal to extend CFIUS to equipment purchases would increase costs for network providers, equipment manufacturers, and ultimately consumers. In addition, it is likely that the responsible federal agencies will also incur additional administrative costs in implementing any supply chain risk management requirements.

Impact on Business Decisions and Competition

All of the approaches may have an impact on the business decisions of network providers and equipment manufacturers and competition within the industry. The Australian government is aware that its proposed framework could have effects on the industry, and it is trying to anticipate

[87] Some of the federal entities we interviewed were not willing to discuss questions about extending CFIUS to network provider purchases of foreign-manufactured equipment.

[88] Australian Government, Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats,* July 2012 and Ofcom, *Ofcom Guidance on Security Requirements in the Revised Communications Act 2003* (February 2012).

[89] Kent Bressie and Madeleine Findley, "Coping with India's New Telecom Equipment Security Requirements and Indigenous Innovation Policies," *Submarine Telecoms Forum,* no. 62 (2012).

these effects and explore how they might be mitigated. It is also seeking input from industry and government stakeholders on any potentially broader effects on competition in the telecommunications market and on consumers.[90] Similarly, a telecommunications industry group reported the Indian requirements complicate the relationship between telecommunications service providers and their equipment vendors, creating concerns about access to intellectual property and giving each an incentive to shift the risk of enforcement onto the other (though the current requirements still place the principal obligations on the licensees).[91] Representatives from a U.S.-based equipment manufacturer told us that extending the CFIUS process to equipment purchases could potentially lead to vendors being excluded from the U.S. market without appeal rights; this would result in limited competition and therefore potentially higher prices for consumers. Similarly, four network providers and one think tank also told us that extending CFIUS to equipment purchases would limit competition and raise costs.

Appropriate Transactions to Include in Procurement Reviews

The appropriate universe of equipment supply contracts that would be subject to review would need to be defined if the CFIUS process were extended to cover these transactions. There were 269 notices of transactions covered by the CFIUS process from 2009 through 2011. By comparison, four network providers and two equipment manufacturers we spoke with noted that network providers conduct thousands of transactions a year and expressed concerns about their being subject to a CFIUS-type process. Specifically, the two manufacturers said it would be difficult for CFIUS members to oversee all of these transactions in a timely fashion, adding expense to the procurement process for network providers and equipment manufacturers that could be passed on to consumers. In addition, CFIUS member agencies may incur significant administrative costs if asked to review thousands of procurement transactions per year.

[90] Australian Government, Attorney-General's Department, *Equipping Australia against Emerging and Evolving Threats* (July 2012).

[91] Kent Bressie and Madeleine Findley, "Coping with India's New Telecom Equipment Security Requirements and Indigenous Innovation Policies," *Submarine Telecoms Forum*, no. 62 (2012).

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

Contact and Acknowledgments

If you or your staff members have any questions about this testimony, please contact me at (202) 512-2834 or goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are listed in appendix V.

Appendix I: Scope and Methodology

We focused our review on the core networks that constitute the backbone of the nation's communications system and the equipment—such as routers, switches and evolved packet cores—that transport traffic over these networks. We also focused on the wireline, wireless, and cable access networks used to connect end users to the core wireline networks. We did not address broadcast or satellite networks because they are responsible for a smaller volume of traffic than other networks.

To obtain information on all of our objectives we conducted a literature review and semi-structured interviews with or obtained written comments from academics, industry analysts, and research institutions; federal entities; domestic and foreign equipment manufacturers; industry and trade groups; network providers; and security and software audit firms as shown in table 5.

Table 5: Individuals and Organizations Selected for Interviews

Stakeholder category	Name
Academics, industry analysts, and research institutions	Center for Strategic and International Studies
	Dr. Diganta Das, Research Staff Center for Advanced Life Cycle Engineering University of Maryland, College Park
	Dr. Sandor Boyson Research Professor & Co-Director Supply Chain Management Center Robert H. Smith School of Business University of Maryland, College Park
	Gartner, Inc.
Federal entities	Department of Commerce
	Department of Defense
	Department of Homeland Security
	Department of Justice, FBI
	Department of State
	Department of Treasury
	Federal Communications Commission
	General Services Administration
	Office of the U.S. Trade Representative
	National Security Agency
	U.S.-China Economic and Security Commission
	U.S. International Trade Commission
	White House national security staff

Stakeholder category	Name
Domestic and foreign equipment manufacturers	Alcatel-Lucent SA
	Cisco
	Fujitsu[a]
	Huawei Technologies
	Intel[b]
	Juniper Networks
	L.M. Ericsson
	Tellabs
	ZTE Solutions
Industry and trade groups	Association of Public Safety Communications Officials
	Communications Sector Coordinating Council
	CTIA – The Wireless Association
	Internet Security Alliance
	The Open Group
	Software Assurance Forum for Excellence in Code
	Telecommunications Industry Association
Network providers	AT&T
	Century Link
	Clearwire
	Cox Communications
	Frontier
	MetroPCS
	Sprint/Nextel
	T-Mobile
	Verizon
	Windstream
Security and software audit firm[c]	Electronic Warfare Associates (EWA)
Foreign countries	International and Regulatory Development Group United Kingdom
	Attorney-General's Department Australian Government

Source: GAO.

[a] At the time of our interview, Fujitsu no longer manufactured routers and switches, but provided aggregation and transport networking equipment.

[b] Intel makes microprocessors that are used in routers and switches.

[c] We attempted to contact McAfee as a security and software audit firm; however, it referred us to Intel representatives since McAfee is a subsidiary of Intel.

We selected the stakeholders based on relevant published literature, our previous work, stakeholders' recognition and affiliation with a segment of the communications industry (domestic and foreign equipment manufacturers, industry and trade groups, network providers and so forth), and recommendations from the stakeholders interviewed. We also spoke with federal entities that have a role in addressing cybersecurity, international trade, and the Committee on Foreign Investment in the U.S. (CFIUS).

To describe how communications network providers and equipment manufacturers help ensure the security of foreign-manufactured equipment that is used in commercial communications networks, we interviewed network providers; domestic and foreign equipment manufacturers (routers, switches, and evolved packet cores); and industry and trade groups. Information we collected included specific industry practices, such as the use of security provisions in contracts; the extent to which domestic and international standards help guide their practices; and any industry-wide efforts addressing supply chain security. We focused this work on the five wireless and five wireline network providers with the highest revenue, the eight manufacturers of routers and switches with the highest market shares in the U.S. market, and two cable network providers. To identify the top five U.S. wireless providers by subscribers, we used data from the Department of Defense and verified the subscribership data against investor relations reports from the providers. To identify the top five U.S. wireline providers by subscribers, we used publicly available rankings and verified the subscriber data against investor relations reports from the providers. We selected the top eight manufacturers of routers and switches based on 2010 U.S. market share. We selected two of the top three U.S. cable companies based on 2011 subscriber data.[1]

To identify how the federal government is addressing the potential risks of foreign-manufactured equipment that is used in commercial communications networks, we asked federal agencies to identify statutes and regulations to identify potential sources of the federal government's legal and regulatory authority over how communications network providers ensure the security of their U.S. commercial networks. Additionally, we interviewed and collected documentation from 13 federal

[1] One of the cable companies did not respond to our request for an interview.

entities to identify related federal efforts, such as interagency information sharing initiatives and those with the private sector.

To determine other approaches, including those of foreign countries, for addressing the potential risks of using foreign-manufactured equipment in commercial communications networks, we conducted a literature review and interviewed stakeholders. We identified other approaches from governmental entities in Australia, India, and the United Kingdom (UK) that address supply chain risks for commercial communications networks.[2] These countries were chosen to show the variation in how foreign governments are approaching supply chain risk management. We also considered criteria such as the availability of public information on the approach to allow for a detailed review and language considerations. While the results of the data collected from these three countries may not encompass all possible approaches, it provided important insights into the approaches that some countries are using to address supply chain risks for commercial communications networks.

We reviewed documents and interviewed officials from governmental entities in Australia, India, and the UK to describe the approaches and issues that could arise from using these approaches.[3] We identified these issues based on interviews with foreign government officials and U.S. industry stakeholders, and our review of foreign proposals and other documentation. The issues identified provide a range of considerations, but is not an exhaustive list of all issues that could be considered.

We also assessed the potential for using the CFIUS review process for purchases of foreign-manufactured equipment because a voluntary notification process similar to CFIUS is being discussed by government and industry stakeholders. We reviewed the Foreign Investment and National Security Act of 2007, related regulations, and CFIUS's annual reports to Congress to describe the CFIUS process. We reviewed CFIUS's transaction data to describe the number of covered transactions, investigations, and Presidential decisions made from calendar years 2009 to 2011 to provide context. Additionally, we interviewed officials from federal agencies and industry stakeholders on how the commercial

[2] We attempted to include Canada in our review, but there was limited public information on its approach and Canadian officials did not respond to our request for an interview.

[3] Indian officials did not respond to our request for an interview.

communications market in the United States may be affected if any of the identified approaches are used when U.S. communications companies purchase equipment manufactured in foreign countries. We conducted data reliability testing to determine that any data used are suitable for our purposes.

We conducted this performance audit from December 2011 to May 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Examples of Threats to the Information Technology Supply Chain

Supply chain threats are present at various phases of the life cycle of communications network equipment. Each of the key threats presented in table 6 could create an unacceptable risk to a communications network.

Table 6: Threats to the Information Technology Supply Chain

Threat	Description and Adverse impact
Installation of hardware or software containing malicious logic	*Malicious logic* is hardware, firmware, or software that is intentionally included or inserted in a network for a harmful purpose. Malicious logic can cause significant damage by allowing attackers to take control of entire systems and thereby read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations' systems; or destroy systems.[a]
Installation of counterfeit hardware or software	*Counterfeit information technology* is hardware or software that contains nongenuine component parts or code. The Defense Department's Information Assurance Technology Analysis Center has reported that counterfeit information technology threatens the integrity, trustworthiness, and reliability of information systems for several reasons, including the facts that counterfeiting presents an opportunity for the counterfeiter to insert malicious logic or backdoors[b] into the replicas or copies that would be far more difficult in more secure manufacturing facilities.[c]
Failure or disruption in the production or distribution of critical products	Disruptions can be caused by labor or political disputes and natural causes (e.g., earthquakes, fires, floods, or hurricanes). Failure or disruption in the production or distribution of a critical product could affect the availability of equipment that is used to support the communication networks.
Reliance on a malicious or unqualified service provider for the performance of technical services	Contractors and other service providers may, by virtue of their position, have access to network hardware and software. As we have previously reported, service providers could attempt to use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.[d]
Installation of hardware or software that contains unintentional vulnerabilities	*Unintentional vulnerabilities* are hardware, software, or firmware that are included or inserted in a network and that inadvertently present opportunities for compromise. The vulnerabilities identified could allow remote attackers to, among other things, cause a denial of service. A "denial of service" is a method of attack from a single source that denies system access to legitimate users by overwhelming the targeted computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.

Source: GAO analysis of unclassified government and nongovernmental data.

Note: NIST defines "information technology" as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes, among other things, computers, software, firmware, and services (including support services).

[a] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

[b] Backdoor is a general term for a malicious program that can potentially give an intruder remote access to an infected computer. At a minimum, most backdoors allow an attacker to perform a certain set of actions on a system, such as transferring files or acquiring passwords.

[c] Information Assurance Technology Analysis Center, Security Risk Management for the Off-the-Shelf (OTS) Information and Communications Technology (ICT) Supply Chain An Information Assurance Technology Analysis Center (IATAC) State-of-the-Art Report, DO 380 (Herndon, Va.: August 2010).

[d] GAO, *Information Security: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data*, GAO-11-308 (Washington, D.C.: Mar. 15, 2011).

Appendix III: Examples of Supply Chain Vulnerabilities

Threat actors can introduce the threats described in appendix II by exploiting vulnerabilities at multiple points in the global supply chain. Table 7 describes examples of the types of vulnerabilities that could be exploited.

Table 7: Examples of Supply Chain Vulnerabilities

Vulnerability	Description	Threat example
Acquisition of network equipment or parts from independent distributors, brokers, or the gray market	Purchasing from a source other than an original component manufacturer or authorized reseller may increase the risk of encountering substandard, subverted, and counterfeit products. Independent distributors purchase new parts with the intention to sell and redistribute them back into the market, without having a contractual agreement with the original component manufacturer. Brokers are a type of independent distributor that work in a just-in-time inventory environment and search the industry and locate parts for customers as requested. The "gray market" refers to the trade of parts through distribution channels that, while legal, are unofficial, unauthorized, or unintended by the original component manufacturer.	Installation of counterfeit hardware or software
Lack of adequate testing for software updates and patches	Applying untested updates and patches to network components may increase an agency's risk that an attacker could insert malicious code of its choosing into a system. For example, if a contractor fails to validate the authenticity of patches with suppliers, an attacker could write a fake patch that might allow unauthorized access to information in the network.	Installation of hardware or software containing malicious logic
Incomplete information on IT suppliers	Acquiring IT equipment, software, or services from suppliers without understanding the supplier's past performance or corporate structure may increase the risk of (1) encountering substandard, subverted, and counterfeit products, or (2) providing adversaries of the United States with access to sensitive systems or information.	Installation of hardware or software containing malicious logic Installation of hardware or software that contains unintentional vulnerabilities Installation of counterfeit hardware or software Failure or disruption in the production or distribution of critical products Reliance on a malicious or unqualified service provider for the performance of technical services

Source: GAO analysis of unclassified government and nongovernmental data.

Appendix IV: Potential Sources of Authority for Taking Action to Ensure Supply Chain Security

In examining potential sources of authority related to supply chain security, we focused on DHS, FCC, and Commerce because of their roles in critical infrastructure protection. Homeland Security Presidential Directive 7 (2003) designated DHS as the sector-specific federal agency for the telecommunications critical infrastructure sector. It required DHS to set up appropriate systems, mechanisms, and procedures to share cyber information with other federal agencies and the private sector, among others. The Communications Sector-Specific Plan of the National Infrastructure Protection Plan characterizes FCC and Commerce as partners that have relevant authority and support DHS's communications critical-infrastructure protection efforts.

Department of Homeland Security

DHS has not identified specific authorities that would permit it to take action to ensure the security of the supply chain of commercial networks. Officials from DHS's Office of General Counsel stated that the Homeland Security Act might have applicable authority,[1] although this authority is not specific to the security of the supply chain of commercial networks. DHS further stated that it cannot say what specific authority it might use if it needed to take action because it has not faced a set of circumstances related to a commercial network's supply chain security requiring action.

Federal Communications Commission

Officials from FCC's Office of General Counsel stated that FCC could regulate network providers' supply chain practices to assure that the public interest, convenience, or necessity are served if circumstances warranted.[2] Specifically, FCC could impose supply chain requirements on providers of common carrier[3] wireline and wireless voice services[4] and, in

[1] 6 U.S.C. §§ 121(d), 131-134, 143. See, also, *Assignment of National Security and Emergency Preparedness Communications Functions,* Exec. Order No. 13,618 77 Fed. Reg. 40,779 (2012).

[2] Under the Communications Act of June 19, 1934, ch. 652, 48 Stat. 1064, codified as amended at title 47, United States Code, the FCC has authority to regulate common carriers providing communications services. See, *also,* 47 U.S.C. §§ 214, 307, 309(a), 316(a).

[3] A communications common carrier, such as a telephone company, provides communications services for hire to the public. 47 U.S.C. § 153(11).

[4] Title II of the Communications Act gives the FCC authority to regulate wireline common carriers. 47 U.S.C. ch 5, subchapter II, Pt. II. Commercial mobile service providers, such as wireless phone service carriers, are also treated as common carriers under Title II of the Act, to the extent they provide common carrier services. 47 U.S.C. § 332(c). Wireless carriers are also subject to regulation as Commission licensees under Title III of the Communications Act.

specific circumstances, information services providers,[5] using FCC's authority under the Communications Act.[6] Officials stated that FCC has not yet attempted to use these sources of authority to impose regulations specifically designed to address cybersecurity threats.

FCC officials stated that because the agency has not adopted regulations or policies related to supply chain security in commercial communications networks, reliance on these sources of authority has not been tested by legal challenges in court. According to FCC officials, legislative changes to the Communications Act to provide express recognition of the agency's authority to address such threats would reduce the risk of such challenges and may facilitate adoption of supply chain security regulation.

FCC officials added that although its current legal authority could allow FCC to act to impose supply chain requirements on network providers, it has not determined the extent to which it has authority to regulate companies that manufacture network equipment. In the past, the agency regulation of equipment manufacturers has focused on interference

[5] Under the Communications Act, an "information service" is defined as the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service. 47 U.S.C. § 153(24).

[6] According to FCC officials, FCC could impose supply chain mandates on wireline carriers Under Title II of the Act. See 47 U.S.C. §§ 201, 214. Under Title III, the Commission has authority to regulate and license radio spectrum, and FCC officials told us that it could impose supply chain conditions on wireless licenses to serve the public interest, convenience, or necessity. See 47 U.S.C. §§ 307, 316. According to FCC officials, the Commission could condition new wireless licenses or modify existing wireless license to impose supply chain requirements, either individually, after allowing the licensee to protest the proposed requirements, or as a class in a rulemaking. See *Committee for Effective Cellular Rules v. FCC*, 59 F.3d 1309, 1319 (D.C. Cir. 1995), In the Matter of *Spectrum and Service Rules for Ancillary Terrestrial Components in the 1.6/2.4 GHz Big LEO Bands*, 22 FCC Rcd. 19,733, 19,743-44 (¶ 23) (2007) (citing *WBEN, Inc. v. United States*, 396 F.2d 601, 617-20 (2d Cir. 1968), *cert. denied*, 393 U.S. 914 (1968)) (examples of the Commission modifying licenses in rulemaking proceedings). With respect to information services, FCC officials told us that the Commission may regulate otherwise unregulated providers of information services, under Title I of the Communications Act, if doing so is reasonably ancillary to the effective performance of the Commission's responsibilities set out in other titles of the Communications Act. In addition, to the extent an information service provider holds any FCC licenses, the agency would have direct regulatory authority over that provider. See *In the Matter of Reporting Requirements for U.S. Providers of International Telecommunications Services* 28 FCC Rcd. 575 (2013), at ¶ 83 (exercising FCC's ancillary jurisdiction).

management. FCC officials told us that they are actively participating in discussions within the executive branch regarding supply side issues, though which agencies should take the lead on this issue has not been determined.

Department of Commerce

Commerce officials stated that Section 232 of the Trade Expansion Act of 1962,[7] as amended, could potentially provide authority for Commerce to use when communications equipment purchases pose a potential risk to national security. According to Commerce documents, Section 232 gives Commerce statutory authority to conduct investigations to determine the effect of imports on national security. If an investigation finds that an import may threaten to impair national security, then the President may use his statutory authority to "adjust imports," by taking measures recommended by the Secretary of Commerce, including barring imports of a product. Commerce has not used, or attempted to use, this authority for any cases involving the communications sector. Commerce officials stated that they reviewed this authority in 2010 in part because a major network provider was considering purchasing foreign-manufactured communications equipment from a company that the federal government believed might pose a national security threat. Since the network provider decided not to purchase equipment from that company, Commerce did not review the potential applicability of Section 232 to that transaction.

[7] Pub. L. No. 87-794, 76 Stat. 872 (1962), codified as amended at 19 U.S.C. ch. 7.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Mark L. Goldstein, (202) 512-2834 or goldsteinm@gao.gov

Contact and Acknowledgments

In addition to the contact named above, Heather Halliwell, Assistant Director; Derrick Collins; Swati Deo; Anne Doré; Bert Japikse; Sara Ann Moessbauer; Josh Ormond; Amy Rosewarne; and Hai Tran made key contributions to this testimony.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.

GAO
Highlights

Highlights of GAO-13-652T, a testimony before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, House of Representatives

May 21, 2013

TELECOMMUNICATIONS NETWORKS

Addressing Potential Security Risks of Foreign-Manufactured Equipment

Why GAO Did This Study

The United States is increasingly reliant on commercial communications networks for matters of national and economic security. These networks, which are primarily owned by the private sector, are highly dependent on equipment manufactured in foreign countries. Certain entities in the federal government view this dependence as an emerging threat that introduces risks to the networks. GAO was requested to review actions taken to respond to security risks from foreign-manufactured equipment.

This testimony addresses (1) how network providers and equipment manufacturers help ensure the security of foreign-manufactured equipment used in commercial communications networks, (2) how the federal government is addressing the risks of such equipment, and (3) other approaches for addressing these risks and issues related to these approaches.

This is a public version of a sensitive report that GAO issued in May 2013. Information deemed sensitive has been omitted. For the May 2013 report, GAO reviewed laws and regulations and interviewed officials from federal entities with a role in addressing cybersecurity or international trade, the five wireless and five wireline network providers with the highest revenue, and the eight manufacturers of routers and switches with the highest U.S. market shares. GAO obtained documentary and testimonial evidence from governmental entities in Australia, India, and the United Kingdom, because of their actions to protect their networks from supply chain attacks.

View GAO-13-652T. For more information, contact Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

The network providers and equipment manufacturers GAO spoke with reported taking steps in their security plans and procurement processes to ensure the integrity of parts and equipment obtained from foreign sources. Although these companies do not consider foreign-manufactured equipment to be their most pressing security threat, their brand image and profitability depend on providing secure, reliable service. In the absence of industry or government standards on the use of this equipment, companies have adopted a range of voluntary risk-management practices. These practices span the life cycle of equipment and cover areas such as selecting vendors, establishing vendor security requirements, and testing and monitoring equipment. Equipment that is considered critical to the functioning of the network is likely to be subject to more stringent security requirements, according to these companies. In addition to these efforts, companies are collaborating on the development of industry security standards and best practices and participating in information-sharing efforts within industry and with the federal government.

The federal government has begun efforts to address the security of the supply chain for commercial networks. In 2013, the President issued an Executive Order to create a framework to reduce cyber risks to critical infrastructure. The National Institute of Standards and Technology (NIST)—a component within the Department of Commerce—is responsible for leading the development of the cybersecurity framework, which is to provide technology-neutral guidance to critical infrastructure owners and operators. NIST published a request for information in which NIST stated it is conducting a comprehensive review to obtain stakeholder input and develop the framework. NIST officials said the extent to which supply chain security of commercial communications networks will be incorporated into the framework is dependent in part on the input it receives from stakeholders. GAO identified other federal efforts that could impact communications supply chain security, but the results of those efforts were considered sensitive.

There are a variety of other approaches for addressing the potential risks posed by foreign-manufactured equipment in commercial communications networks, including those approaches taken by foreign governments. For example, the Australian government is considering a proposal to establish a risk-based regulatory framework that requires network providers to be able to demonstrate competent supervision and effective controls over their networks. The government would also have the authority to use enforcement measures to address noncompliance. In the United Kingdom, the government requires network and service providers to manage risks to network security and can impose financial penalties for serious security breaches. While these approaches are intended to improve supply chain security of communications networks, they may also create the potential for trade barriers, additional costs, and constraints on competition, which the federal government would have to take into account if it chose to pursue such approaches.

Mr. WALDEN. Thank you, Mr. Goldstein. We appreciate the work of your team and you——

Mr. GOLDSTEIN. Thank you.

Mr. WALDEN [continuing]. And we appreciate your being here.

I will now go to Mr. Stewart A. Baker who is a partner in Steptoe & Johnson, LLP, and we appreciate your being here and look forward to your comments, sir. Go ahead.

STATEMENT OF STEWART A. BAKER

Mr. BAKER. Chairman Walden, Ranking Member Eshoo, members of the committee, it is a pleasure to be before you again. I was at the Department of Homeland Security and in charge of the CFIUS process until 2009, so I have been here before to talk about that.

I would like to start with the problem that we have. We are under massive cyber espionage attacks. There is no one who is immune against these attacks. I am willing to bet that everybody on this panel and everybody on the committee has already been the subject of intrusions aimed at stealing secrets on behalf of the People's Liberation Army or some other foreign government.

We do not know how to keep people out of our systems effectively. And that is despite the fact that we have, by and large, an IT infrastructure that is designed by U.S. companies who are doing their best to give us security. We simply have not been able to find all of the holes in the code or all of the flaws that can be exploited. That is with the best will in the world.

At the same time, in the last 20 years, I think, as the President's efforts to name and shame China and other attackers have demonstrated, there is plenty of name but not a lot of shame on the other side. This has been an enormously productive intelligence source and it is an enormous weapon that can be used against the United States if we get into a shooting war that our adversaries would like to get us out of. Everything that can be exploited for espionage purposes can be exploited for sabotage purposes.

Our systems can be made to break causing great harm to Americans, including potentially deaths here. And we will have to face that prospect in the next serious conflict that we face internationally because the ability to cause that harm is moving down the food chain to the point where Iran and North Korea are significant powers in causing this harm.

So that is the situation that we face. The question is we are deep in a hole. Are we going to stop digging? And here is the question that we need to face as we look at our supply chain. If American companies looking at their own code and trying to give us security can't find a way to do that, how comfortable are we having companies from countries that are not our friends provide the code, provide the hardware? We are not going to find those problems. We can't even find all of them in the products that we make ourselves here in the United States, as witnessed through all of the exploitable vulnerabilities we face.

And so we face the prospect that some of this equipment simply is not going to be safe. As we have asked ourselves, how do we deal with that problem? It turns out that our tools for dealing with it are remarkably limited. I ran the CFIUS process; I ran the team telecom process for DHS. Those are very limited tools. CFIUS only applies if somebody buys something. If they want to sell something here, there is no restriction whatsoever. So telecommunications gear can be sold in the United States without any review whatsoever.

We got to the point, I think, actually in the stimulus bill where we had provided subsidies to buy telecommunications equipment to carriers and they were buying, with our money, Huawei and ZTE gear because we had no way to prevent that, but at the same time that the U.S. Government was telling Verizon and AT&T don't you buy that stuff. So we clearly lack an ability to address the problem of infrastructure equipment being sold to the United States that we don't think is secure. That is the first thing that I think the committee should examine.

Beyond that, I think we have also discovered as we have begun looking at this problem that our procurement laws do not take into account sufficiently supply chain risk, do not require that our contractors take enough account of supply chain risk. So if there were two things that I would urge the committee to address, it is, one, the limited nature of team telecom and CFIUS remedies and the still remarkably limited ability of government procurement officers to take account of this risk.

[The prepared statement of Mr. Baker follows:]

Cybersecurity: An Examination of the Communications Supply Chain
Statement of Stewart A. Baker
Partner, Steptoe & Johnson LLP
Former Assistant Secretary for Policy, Department of Homeland Security
Former General Counsel, National Security Agency

Before the Committee on Energy and Commerce
Subcommittee on Communications and Technology
U.S. House of Representatives

May 21, 2013

Chairman Walden and Ranking Member Eshoo, I appreciate the opportunity to provide this statement today.

Protecting the information and communications (ICT) supply chain is not a new problem. It was a concern in the 1990s when I was General Counsel at the NSA; it had become far harder when I was Assistant Secretary for Policy at the Department of Homeland Security in 2005-2009. But it has never been more important or more difficult than it is today.

1. The Threat

I hope that there is no need to dwell on the unprecedented wave of cyberattacks that the United States has suffered in recent years. Intrusions on our networks have reached new heights. They have moved from penetration of government and military systems to wholesale compromises of companies, trade associations, think tanks, and law firms. Most of these attacks have been carried out for espionage purposes – stealing commercial, diplomatic, and military secrets on a massive scale.

This espionage campaign has paid dividends for our adversaries, and it's likely to pay more, because any network that can be compromised for the purpose of espionage can be compromised for the purpose of sabotage. The next time we face the prospect of a serious military conflict, we can expect our adversaries to threaten the destruction of computer networks – and the civilian infrastructure they support – inside the United States, probably before we have fired a shot. From the American point of view, this is a new and profoundly destabilizing vulnerability. From our adversaries' point of view, it is an exciting new weapon with enormous potential to neutralize many of our traditional military advantages.

To make things worse, one of the countries that the Obama administration has criticized most often for cyberattacks, China, is also a major supplier of increasingly sophisticated electronic equipment to the United States. Given the value of cyberespionage for waging both war and peace, it's only reasonable to assume that every potential adversary asks itself whether it can make the job of its cyberwarriors easier by tinkering with electronic gear before it's shipped to the United States. Or, as I put it in *Skating on Stilts*, a book about technology challenges to policymakers, if the "countries that [view] us as an intelligence target … could get their companies to compromise U.S. networks, they'd do it in a heartbeat."

That, at least, has not changed. And it is the most troubling supply chain problem we face.

But there's another that is also of concern. As electronics producers diversify their suppliers to the global lowest bidder, the risk grows that some of those suppliers will be irresponsible, cutting corners on quality or actively substituting inferior parts to boost profits. If our military electronics fail in a crisis, it matters little whether the failure was caused by deliberate sabotage or a bad outsourcing decision.

Either way, the security of our electronics supply chain is critical.

2. Partial Regulatory Authority -- CFIUS and Team Telecom

For policymakers, threats to the supply chain have most often arisen when foreign companies purchase U.S. suppliers. That's because U.S. law requires a national security review of such acquisitions by the Committee on Foreign Investment in the United States, or CFIUS. When I ran CFIUS, we aggressively used our authority to negotiate "mitigation" agreements with foreign purchasers to reduce the supply chain risk, something I discussed in *Skating on Stilts*:

> [A]llowing foreign companies to take up critical positions in U.S. computer and telecommunications networks, either as suppliers or as service providers, raised serious national security issues. At the same time, globalization was relentless. The old days, when AT&T provided local and long distance service—and made all the equipment on the network—were long gone. And the collapse of the high-tech bubble had transformed the industry that emerged from AT&T's breakup. The Baby Bells were consolidating; long distance was disappearing as a separate business; wireless was displacing land-lines; and the equipment companies that had dominated North America for a century were in trouble. We couldn't just say no when foreign companies came courting. In that context, mitigation agreements became a way to say yes to globalization without completely surrendering to foreign espionage. The agreements became a kind of company-specific network security regulation. We began to insist on a mitigation agreement in any transaction that posed even a modest threat. Each agreement created an ad hoc regime designed to curb foreign government infiltration of U.S. telecommunications and information technology. . . .
>
> [A] common security measure was to insist that the government (or an approved third party with technical skills) be guaranteed the right to inspect the buyer's hardware designs and processes, its software source code and testing results, and any other part of the production process that might reveal a deliberate compromise. To make sure that data was not shipped abroad and compromised there, some mitigation agreements required that data about Americans be kept in the country; sometimes the agreements required special security measures for the data….

> We were acutely aware that these measures weren't perfect. ... In theory, access to source code and hardware designs would allow our experts to find any Trojan horse built into the product. But few government workers have the expertise to find these needles in a haystack of products. Unless we insisted that the companies pay for very expensive outside experts to check their work, or we received an intelligence tip about corporate misbehavior, we had only a modest chance of catching a really clever compromise. ...
>
> Still, imperfect as they were, mitigation agreements were well ahead of whatever was in second place. They were in fact our only good tool for policing foreign efforts to build insecurity into U.S. networks.

Though there has been progress, it remains true that CFIUS remains one of the few tools that the U.S. government can use to address supply chain risk, especially in telecommunications and information technology.

The mitigation agreements themselves continue to expand in scope as new threats emerge. For example, where it was once enough to insist that telecommunications data and control be kept under U.S. control by maintaining a Network Operating Center in this country, officials have come to recognize that such centers are filled with equipment that must be updated and maintained remotely by the equipment supplier, opening new avenues for compromise. CFIUS agreements now must be concerned not only about foreign companies managing traffic on U.S. networks, but also about the equipment that comprises these networks and the vendors that supply that gear.

But the hard fact remains that CFIUS is an inadequate tool for this job. It gives the government only haphazard insight and leverage over the security of telecommunications and information technology. That's because CFIUS has jurisdiction only over corporate acquisitions. Team Telecom, which I also oversaw from a DHS perspective, adds a bit to that authority, giving national security agencies an ability to impose conditions on foreign telecommunications carriers seeking Federal Communications Commission licenses to operate in the United States. But Team Telecom has no explicit authority in law; its reach is no greater than the FCC's. As a result, even the most dangerous and unreliable suppliers of commercial telecom and IT equipment are free to sell their products in the United States without an inquiry into the security risks the products may pose.

Even recently adopted programs such as federal government subsidies for rural wireless service and "smart grid" deployments – programs embraced in the American Recovery and Reinvestment Act of 2009 – have no statutory provisions to ensure that federal dollars are not spent on equipment that will impair national security. And Section 232 of the Trade Expansion Act of 1962, which allows the President to restrict imports that threaten to impair national security, [1] has never been applied outside the importation context. While news reports indicate

[1] 19 U.S.C. § 1862. The Supreme Court has upheld broad use of section 232 to restrict imports. *See Federal Energy Administration v. Algonquin SNG, Inc.*, 426 U.S. 548, 564 (1976) (Section 232 authorizes the President "to take whatever action he deems necessary to adjust

that the Commerce Department successfully dissuaded Sprint from awarding a large contract to Huawei, there may be no statutory basis to do so where the contract does not involve importation of products.

3. A Patchwork Quilt of New Measures

That said, the last few years a growing number of government and private-sector stakeholders have taken action to "harden" the ICT supply chain. It is hard to call the resulting measures anything but a patchwork quilt of remedies. There are no standard or consistent practices, and monitoring and verification tools are limited. Significant gaps continue to exist in U.S. policy, and no single U.S. government agency or organization is responsible for supply chain security. (For a good, recent summary of overall supply chain vulnerabilities, I recommend *Remaking American Security*, prepared by former Gen. John Adams for the Alliance for American Manufacturing.) Federal procurement law and policies in particular are struggling to come to grips with ICT supply chain challenges. Nonetheless, these new measures represent a series of experiments and tentative steps that may yet lead to a more comprehensive approach.

Securing Critical Infrastructure

The vast majority of critical infrastructure is privately owned and operated. These owners generally are free to use whatever vendors and supply chains they prefer. Securing government systems is hard enough, but how are we to secure supply chains for privately owned critical infrastructure? This is among the hardest of the hard problems.

A cybersecurity Executive Order issued in February of this year is a decent start. It calls for the development of a cybersecurity framework that critical infrastructure and other U.S. companies will be encouraged or required to adopt.

Due to be published in February 2014, the framework likely will create a basis for official communications discouraging the use of products from untrusted sources and from service providers who depend on such sources. For example, the framework likely will encourage companies to adopt procedures to vet vendors and suppliers from the perspective of cybersecurity risk.

Because large swaths of the U.S. economy are critical infrastructure – including many energy, telecommunications, and transportation companies – this guidance could have a broad impact.

While the Framework likely will not impose mandatory requirements or exclude particular vendors, they may create a mechanism by which security warnings are incorporated into private company security practices. With the Framework in place, critical infrastructure owners are less likely to ignore government warnings about relying on untrustworthy foreign

imports . . . [including the use of] tariffs, quotas, import taxes or other methods of import restriction.") (*quoting* 101 Cong. Rec. 5299 (1955) (statement of Sen. Millikin)).

telecommunications equipment providers. If a telecommunications network fails, and calls or emails are disrupted for an extended period of time, the telecommunications company may have to defend the "reasonableness" of its actions in court. If that company ignored government warnings by purchasing untrustworthy equipment, that defense would be a steep, uphill struggle. And that prospect should cause infrastructure owners to heed government warnings.

Government Contracts

Considerable attention has been focused on the threat that untrustworthy products pose for government procurements. The Department of Defense (DoD) has made the most explicit effort to address ICT supply chain security risks by incorporating cybersecurity requirements into acquisition planning and contract administration. Similarly, the National Institute for Standards and Technology (NIST)—which sets information government-wide security standards— has instructed agencies to develop acquisition policies to protect against supply chain threats.

The point of these efforts is to protect mission-critical components, whether hardware, software, or firmware. Suggested protective measures include: (1) withholding the ultimate purpose of a technology by using blind or filtered buys, so that the vendor does not know how the components will be used; (2) additional vetting of the processes and security practices of subordinate suppliers; and (3) restricting purchases from specific suppliers or countries.

To implement this guidance, agencies have begun training contracting officers on cybersecurity requirements and inserting clauses into procurement documents that allow them to disqualify bidders because of supply chain and other security concerns. Going forward, this trend is likely to change the ways in which the government, and its contractors, source procurements.

Much of the focus on government procurement practices has been driven by Congress. For example, Section 852 of the 2012 National Defense Authorization Act (NDAA) requires DoD to map the supply chain for critical items from raw material to final products. The legislation also requires DoD to perform a risk assessment of the supply chain for such items. The FY11 NDAA permits DoD to exclude a particular source that presents an unacceptable level of supply chain risk, and withhold certain information regarding the basis of that decision. The FY12 Intelligence Authorization Act allows members of the intelligence community to do the same.

Recently, a number of congressional hearings and reports, and in some cases specific statutory language, have highlighted the ICT supply chain risk from China in particular and led to a strengthening of restrictions on Chinese products. To take one example, Section 516 of the FY2013 Continuing Resolution bans the Departments of Justice and Commerce, NASA, and National Science Foundation from acquiring IT systems "produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China." This prohibition, though not yet implemented, represents a significant change in the IT procurement process, and it raises the likelihood that similar prohibitions could be imposed throughout the federal government.

Indeed, similar bills are pending. The Deter Cyber Theft Act, for instance, would require the Director of National Intelligence to produce an annual report that lists which foreign countries conduct cyber espionage against American companies or individuals, as well as technologies targeted by cyber spies. Additionally, the bill would require the president to block imports of products containing technology siphoned from the United States.

4. Recommendations

Virtually everyone recognizes that this ICT supply chain security problem is hard and that the "solutions" to date have been ad hoc. Nevertheless, both government and private-sector stakeholders appear to have agreed on a number of common best practices. These include:

- Prioritizing efforts to secure the most important and sensitive systems (especially National Security Systems);
- Use of procurement tools to drive security improvements;
- Use of intelligence community assessments to inform mitigation strategies;
- Development of standards drawn from actual commercial practice wherever possible;
- Finding ways for the government to share specific and contextual threat information; and
- Using technical tools and engineering solutions to mitigate risk.

Of these six common elements, three seem to me to be especially significant for government policymaking (via legislation and/or otherwise). At a minimum, we should consider legislation or executive action encouraging:

1. The use of procurement tools, especially by writing additional supply chain security requirements into procurement contracts, and educating procurement officials about which contracts need these requirements.

The need for supply chain security does not apply just to DoD and security agencies. Many agencies – and private companies – need better information about the provenance of the products that they rely upon. More government agencies should require that contractors and subcontractors develop and submit supply chain security plans that include ICT supply chain specific risk assessments. This will both help prioritize security measures and ensure these measures are consistent with a cost-effective approach. As a guiding principle, the security mechanisms should be more robust depending on the sensitivity of the system, component, or information at issue.

At a minimum, the government should implement mandatory supply chain security training and education for contracting officers and other procurement officials. Without such comprehensive and routine training, government officials will be ill-equipped to adequately understand and evaluate supply chain risk with respect to individual contract vehicles.

2. Additional reliance on intelligence community assessments regarding supply chain risks, with some mechanism to share that information with U.S. Government contractors and other critical infrastructure providers, as warranted, without fear of endless litigation.

The DNI's Office of the National Counterintelligence Executive (NCIX) has developed a common methodology for conducting threat assessments on entities that do business with the national security community. These classified assessments should continue to inform supply chain security decisions and they should be shared, as appropriate, with industry partners.

I have discussed this idea over the years with various members of the intelligence community, and it never takes long before I hear some variation of, "We can't do that. If we say something bad about a particular company, we'll get sued." If Congress wants to encourage better sharing of threat information, it should devote less attention to the problem of clearances for private sector companies, which I think has largely been solved, and more attention to the problem of how to protect sources and methods while also creating a limited, effective remedy for companies that believe that they have been treated wrongly in a threat assessment.

3. Incorporating technical protections and redundancies into products and systems exposed to supply chain risks.

For some information system components, especially hardware, technical means are available to determine if components have been subjected to tampering. There are also trusted/controlled distribution, delivery, and warehousing options, such as requiring tamper-evident packaging of information system components. The government should look to industry for these solutions and incorporate them into best practices guidance.

Beyond these patches, the federal government may need authority to take action to stop an urgent national security threat relating to the compromise of our supply chain. The embarrassing spectacle of one part of the U.S. government subsidizing small carriers' purchases of foreign equipment at the same time that it is warning large U.S. carriers not to buy the same equipment suggests that we simply do not yet have sufficient legal authority to respond to supply chain threat outside of the CFIUS context.

Mr. WALDEN. Mr. Baker, thank you for your testimony.

We are going to go now to Jennifer Bisceglie, who is President and CEO of Interos Solutions, Incorporated. We welcome you and look forward to your comments.

STATEMENT OF JENNIFER BISCEGLIE

Ms. BISCEGLIE. Thank you. Good afternoon, Mr. Chairman and members of the subcommittee.

Mr. WALDEN. I am going to have you move that microphone a little closer and make sure the light is on.

Ms. BISCEGLIE. It was on.

Mr. WALDEN. OK.

Ms. BISCEGLIE. Can you hear me now? Good afternoon, Mr. Chairman and members of the subcommittee. My name is Jennifer Bisceglie, President of Interos solutions. Thank you for inviting me to testify on behalf of our industry peers focused on supply chain risk management, or SCRM, as we like to call it.

My company Interos is built on 20 years of global supply chain and IT implementation experience. Over the past 6 years, we have seen the discussions turn from simple compliance to resiliency, which is ensuring business operations would continue even if the supply chains were interrupted; and now to product integrity, which is caused by a manmade malicious attack.

In response to this, Interos has set up a SCRM global threat information Center, which offers capabilities to help both the public and private sector organizations implement SCRM frameworks, conduct supplier audits, and conduct open-source research to identify potential threats with current or future suppliers.

I will first share some of our observations and then follow those with some recommendations. First, a common definition for supply chain risk management and cyber security does not exist, nor is there a standard way to measure either challenge. To us, the definition of cyber security extends deep into the supply chain as cyber capabilities are increasingly reliant on globally sourced, commercially produced information technology and communications hardware, software, and services.

To us, cyber security means transparency of where things are coming from, where they are going to, and who has access to them along the way. That is also the definition of supply chain risk management.

Our second observation is that supply chain risk management must be viewed as an investment versus an expense. Interos is working with the Department of Energy on their enterprise SCRM program. With only three Interos team members supporting the entire Department of Energy enterprise, they have an infrastructure they can share resources and information throughout their entire enterprise now.

In this case, it is a relatively low-cost investment and yields tremendous benefits. Much of the success of this program can be attributed to a strong DOE leadership, as well as having the ability to work with the Department of Defense's trusted systems and network SCRM roundtable and their interagency working groups.

Third, we feel supply chain risk management is successful when it is a cultural shift that supports current business process and reduces the need to develop new stovepipe processes that increase costs and create additional work for the risk owner. It is not an issue of being too expensive to do it. It is an issue of being too expensive to ignore it.

Now to our recommendations: from our perspective, Congress can take four steps to better protect our Nation's critical infrastructure. First, awareness and education has to start at the top in order to be adopted by those actually executing the mission. In our experience, the level of awareness of the challenge varies across federal agencies, as does their level of attention to managing their supply chain risk. Awareness and education is critical to communicate that supply chain risk impacts everyone within the federal infrastructure.

Second, fund the program, assign someone within each agency to own the issue, and measure the success. We have seen SCRM focal points, as directed by the Bush and the Obama Administrations, being implemented in different areas within the agencies. Without the top-down support within the agency, without an owner of the concern, and without funding, these programs are being bootstrapped and implemented in various fashions, not conducive to effective protection.

Three, the low-cost, low-price technically acceptable environment is in direct opposition to a safe and secure critical infrastructure unless we are able to accurately define our acceptable supply chain risk tolerance at the beginning of an acquisition cycle. While we understand the federal budget constraints and the temptation to fund program objectives with simply the lowest bid, when it comes to cyber security, it is not a good strategy. Failure to protect our critical infrastructure and educate risk owners on the threats that are brought into an organization by buying from unverified sources will result in continued and increasingly harmful attacks.

Last, implement contractual language that works. We understand that as part of Executive Order 13636, GSA, NIST, and DOD are working with potential recommendations to update the FAR language. In addition, there are multiple industry associations working on standards for supply chain risk management. Doing as much as possible via internal policy changes and contractual language as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization is a much less expensive way to approach the problem than regulation and legislation.

In conclusion, the solution needs to be viewed as an investment in national security, not just another expense. The key for industry and government is to work separately on their internal enterprise risk tolerance levels through good business practices, including awareness training and contractual agreements. This will enable each to meet collaboratively and have informed discussions about where vulnerabilities lie and what it will take to protect our country.

Thank you for the opportunity to present our views. I look forward to answering any questions.

[The prepared statement of Ms. Bisceglie follows:]

Executive Summary

Statement of Jennifer Bisceglie

President

Interos Solutions, Inc

Before the

Subcommittee on Communications and Technology

Committee on Energy and Commerce

U.S. House of Representatives

May 21, 2013

Interos Solutions, Inc, a woman-owned small business, is built on 20 years of global supply chain and IT implementation experience. Interos predicted this growing wave of concern over cyber security and were at the forefront of leading the cyber-supply chain discussion within government and industry.

Summary of the major points of my testimony:

- Awareness and Education needs to be universal and started at the top of an organization in effort to be adopted by those actually executing the mission.
- Fund the program, assign someone within each agency to 'own' the issue, and measure the success.
- The lowest-price technically acceptable environment is in direct opposition to a safe and secure critical infrastructure.
- We Need Contractual Language That Works. The private sector is looking for the Federal Government to come out with contractual language that they can work with. Doing as much as possible via internal policy changes and contractual language, as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization, is a much less expensive way to approach the problem than regulation and legislation.

Statement of Jennifer Bisceglie

President

Interos Solutions, Inc

Before the

Subcommittee on Communications and Technology

Committee on Energy and Commerce

U.S. House of Representatives

May 21, 2013

Good morning Mr. Chairman and Members of the Subcommittee. My name is Jennifer Bisceglie, President of Interos, Inc. Thank you for inviting us to testify on behalf of our industry peers focused on supply chain risk management or SCRM.

My company, Interos, is built on my 20 years of global supply chain and IT implementation experience. We have had the opportunity to see many waves of compliance and security implemented during our careers – from the initial application of bar codes to boxes, to more sophisticated RFID, and the heightened requirement for advanced shipment notification. These compliance requirements were put in place to help with quality assurance, ensuring the right labor was in place to unload shipments at the customer's delivery site, and provide end-to-end visibility within the supply chain.

The concern for today's discussion, the cyber threat in the supply chain, began bubbling up about six years ago, building to the fever pitch we see today. Interos predicted this growing wave of concern and were at the forefront of leading the discussion within government and industry. The discussions turned from simple compliance to resiliency – ensuring the business operations would continue even if the supply chain was interrupted. Now the issue has morphed the supply chain risk management concept into a combination of resiliency and product integrity caused by an actual man-made attack. In response to this, Interos is again on the forefront of our peers, having stood up a SCRM Global Treat

Information Center that offers capabilities to help both public and private sector organizations implement SCRM frameworks, conduct supplier audits, and conduct open source research to identify potential threats with current or future suppliers.

The lexicon of supply chain risk management is brought up often – a common definition does not exist. Neither does a standard definition of cyber security exist. To some government entities, cyber security is technical and only refers to systems being hacked. To some private entities, cyber security is something they don't need to worry about as they're not big enough for anyone to want anything from. To me, the definition of cyber security extends to the supply chain vs. just IT security. Cyber security means where things are coming from, where they are going to, and who has access to them along the way. That is also the definition of supply chain risk management. Now, we've consolidated resiliency of the supply chain, i.e. what to do if a tsunami hits, into the same bucket as product integrity within the supply chain, i.e. getting the product that you ordered, protected from malware, counterfeits, and back doors into our National Security Systems. In industry, this is another hazard we're carefully watching and are finding the right avenues to protect ourselves.

Another point we would like to bring up is the cost of implementing supply chain risk management mitigations and countermeasures. Supply chain risk management needs to be viewed as an investment instead of expenditure. Interos has had the opportunity to work with the Department of Energy (DOE) on their enterprise SCRM program. They have stood up a Focal Point, which is the hub of their SCRM expertise. With only three Interos team members supporting the DOE Focal Point Program Manager; they have an infrastructure that can share resources and information throughout the entire enterprise.

Interos has taken the stance that the best supply chain risk management practices are implemented in the current workflow – in everyone's day to day job. With this approach, the increased security is cost effective and is viewed as an investment not an expense. This approach is more of a cultural shift that supports current business processes and reduces the need to develop new stovepipe processes that increase cost and create additional work for the risk owner. If SCRM costs too much, or if it is seen as 'another thing people have to do,' it will not be adopted by the stakeholders or user community.

From our perspective, Congress can take four steps to protect our Nation's critical infrastructure.

- **Awareness and Education needs to be universal and started at the top of an organization in effort to be adopted by those actually executing the mission.** In working with Federal agencies across the spectrum from the Intelligence Community, DoD, and .Gov, the level of awareness of the challenge varies across the Federal Agencies. Similarly, so does their level of attention to managing their supply chain risk. Awareness and education is critical to communicate that supply chain risk impacts everyone within the Federal infrastructure. It may be a different level for DOE than for Department of Education, but they are both impacted. At this time, there is not a common level of understanding across the Federal agencies. We see the same varied level of attention and understanding in the private sector. Resiliency has departments stood up and focused on it, normally within an organization's supply chain arm. The amount of attention paid to cyber-supply chain issues depends on where you exist in the supply chain, i.e. manufacturer (being the highest as they care the most about brand and product integrity) down to distributor and customer, where the main focus is financial, i.e. revenue and cost.

- **Fund the program, assign someone within each agency to 'own' the issue, and measure the success –** We have seen RFPs come out various agencies with a myriad of SCRM requirements. We have also seen focal points, as directed by the Bush and the Obama Administration, being implemented in different areas within the agencies. We all agree that the ultimate responsibility – or acceptance of risk – remains with the risk owner, which in the case of the federal government is the program manager. Having said this, without the top-down support within the agencies, without an 'owner' of the concern (being supply chain risk management) and without funding, these programs are being bootstrapped and implemented in various fashions. I understand the budget issues we have as a Federal Government. But with the implications that a breach will significantly impact National Security, it seems to us that funding for cyber-supply chain risk management is an investment the Federal Government needs to make because it is an investment in future security challenges. The private sector is working through many of the same issues, as the protection of the cyber-supply chain crosses the technical into the operational workforce.

- **The lowest-price technically acceptable environment is in direct opposition to a safe and secure critical infrastructure** – While we understand the severely constrained federal budget and the temptation to fund program objective with the lowest bid, when it comes to cyber security, this is not a good strategy. As I mentioned earlier, the federal government needs to see this as an investment in the future of our government's critical infrastructure. Failure to protect our critical infrastructure and educate risk owners on the threats that are brought into an organization by buying from unvalidated sources, will result in continue and increasingly harmful attacks. We see them daily – some are mere nuisances, some are stealing personally identifiable information (PII), corporate espionage, or worse. Manufacturers have a need for good distribution networks and are spending money, annually, to ensure those network distributors are handling their products appropriately. Using certified vendors and distributors provides at least a minimum level of assurance that the products deployed across the critical Federal Infrastructure are authentic. Procurement for those products or components that support our critical infrastructure should always be evaluated with the strictest adherence to industry standards. Lowest price, technical acceptable competition adds additional risk to our Nation's critical infrastructure and should not be an acceptable model for these types of procurements.

We do understand there are acquisitions that do not relate to our Nation's critical infrastructure. In our mind, and from a common sense standpoint, each acquisition needs to be looked at independently, as well as with other systems it may interface with, to assess the risk tolerance of the organization– and the level of supply chain risk management rigor that must be applied to each acquisition. It is too expensive to try to protect everything – and we're not proposing this. But there are easy ways to prioritize what process or functions are critical to an organization, and what systems are supporting those functions. From there, there are processes to drive the conversation down to the components of the systems – which provides you a list of suppliers you need to work with.

- **Contractual Language That Works** – The private sector is looking for the Federal Government to come out with contractual language that they can work with. We understand that as a part of Executive Order 13636, GSA, NIST, and DoD are working with potential recommendations to update the FAR language. In addition, there are multiple industry associations working on standards for SCRM that can be spread across the cyber-supply chain risk management focused community. This will initially increase costs to the private sector and the government purchasers, but if done correctly, should spread the costs over the supply chain as purchasers understand what level of rigor each acquisition requires and the private sector learns how to build that into its cost structure. The increase in cost to the private sector may include additional layers of security, which are Government customer specific, and are not part of their current corporate Cybersecurity policies.

As long as the business case can be made, the two parties will be able to walk through the economics of it. As more informed discussions take place, we will come to the realization that many of us, both in the public and private sector, have the same vulnerabilities that our supply chains need to be secured against. Doing as much as possible via internal policy changes and contractual language, as a way to inform suppliers of how to do business with you and to mitigate risks coming into your organization, is a much less expensive way to approach the problem than regulation and legislation.

We see the adoption of many of these increased security practices being very similar to how bar-coding was adopted back in the 1990's. The big box retailers would charge the manufacturer money if the boxes were not marked correctly, or if the advanced shipment notice had not been received in time for the retailer to plan their dock labor. There was an initial outcry and then the private sector learned to spread the cost and absorb it. We are not asking for anything that will go away any time soon – the standards that are being created right now for SCRM are here to solve a problem that will only become more prevalent.

The topic of information sharing has been brought up repeatedly, and is a large part of the Executive Order 13636. This needs to be encouraged and enabled – not legislated and mandated. What we are seeing in the private sector is that organizations are open to sharing given a level of trust across all vendors and distributors within the supply chain. If the Federal Government took some of the steps above, and provided the private sector with a dependable and repeatable SCRM position, trust will grow between the public and private sectors.

Can we all improve our security practices? Yes we can. The private sector can do a more rigorous job and still remain profitable. That said, the Federal Government needs to own its own problem, starting with adoption of a common level of understanding that this threat is here, it is an important investment, and collectively a solution needs to be crafted. The argument that over 75% of Federal acquisitions are commercial-off-the-shelf (COTS) products, thereby throwing the responsibility over the fence to the private sector does not work. Federal agencies should be able to articulate their level of risk tolerance, and have processes and funding in place, to acquire products based on that information.

For our final point, we would like to stress the far-reaching nature of this threat. Although much of today's conversations, as well as that of the Federal Government and their contractor base's focus, are on information communications technology (ICT) that supports our nation's critical infrastructure, the cyber-supply chain risk issue is all inclusive. It is Interos' position that anyone that purchases technology should look at where they are sourcing from, and how they are using the technology. We used the comparison of DOE vs. Dept of Education earlier – we are sure that although no classified systems may be used, the Dept of Education has information that needs to be protected. By instituting some of the ideas laid out in the four bullets above, both the public and private sector can make some low cost, high value changes in their business processes which will create more security in their supply chains.

We, at Interos, feel the threat is real for every agency and one we should all take very seriously.

Conclusion

Due to Interos' unique position in the marketplace, we have had the opportunity to see the past and current situation of SCRM from multiple perspectives.

We call to your attention a quote from the *National Strategy for Global Supply Chain Security* (January 2012), which states *'We reject the false choice between security and efficiency and firmly believe that we can promote economic growth while protecting our core value as a nation as a people.'* The solution needs to be viewed as an investment in national security, not just another expense. The key is for industry and the government to separately work on their internal risk tolerance levels through good business practices, including awareness, training, and contractual agreements. This will enable each to meet collaboratively, and have informed discussions about where vulnerabilities lie and what it will take to protect our country.

The enemy is smart and persistent but not unstoppable. If we invest the time, use common sense, and work together to improve the government's cyber-supply chain security business practices, our national security will be greatly enhanced.

Thank you for this opportunity to present our views. I look forward to answering any questions.

Mr. WALDEN. Thank you very much for your testimony.

We will now go to Mr. Robert B. Dix, Jr., Vice President of Government Affairs and Critical Infrastructure Protection, Juniper Networks, Incorporated. Mr. Dix, pull that microphone right up and thanks for being with us today. We look forward to your testimony.

STATEMENT OF ROBERT B. DIX, JR.

Mr. DIX. Good afternoon, Chairman Walden, Ranking Member Eshoo, and members of the subcommittee. Thank you for inviting me to be a participant in today's hearing on the security of the communication supply chain.

As indicated, my name is Bob Dix and I serve as the Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks, a publicly held private corporation headquartered in Sunnyvale, California, in Congresswoman Eshoo's district.

I will attempt to address three aspects of this important subject of security and integrity of the communication supply chain: first, the risk created by government procurement practices utilizing unauthorized equipment providers; second, supply chain integrity initiatives by industry; and third, several recommendations where the government can help improve both government and private sector supply chain integrity.

The government views its commercial supply chain rightly as a major element in its risk profile, but many of its risk management efforts are not coordinated and were not developed in collaboration with industries that share legitimate concerns about supply chain security. Today, there are more than 100 different initiatives around supply chain in the government.

Also as we sit here today, the government continues to make purchases from untrusted and unauthorized sources. The urge to save money pushes agencies to brokers and other gray market suppliers that are not part of the authorized or trusted supply chain for original equipment manufacturers. This is in also an area where much mischief takes place for both counterfeiters and those attempting to penetrate the government supply chain with malicious intent.

Interestingly, when the government purchases equipment and then identifies it as counterfeit, it often assumes the OEM has a gap in its supply chain, pointing fingers at the private sector when in many cases they need to be looking in the mirror. The government does not instead ask why it bought sensitive ICT products from an untrusted source.

I have included in my written statement several real-life examples just that Juniper Networks has experienced which are illustrative of this challenge, but time today does not permit me to go through each one of those. But I hope you will take a chance to look at those.

While Juniper understands the importance of improving supply chain assurance for the Federal Government, it often appears that the government itself does not understand the enormous investment that many in the private sector make to protect the integrity of their supply chain. It is in our business interest. It is a market differentiator. Juniper, like many companies, has a supply chain assurance and brand integrity program for securing our products and supply chain. We employ best practices for security from organizations including the Open Groups, Trusted Technology Forum, AGMA, and Safeco to name a few. This includes component integrity, traceability of products, anti-counterfeit measures, and much more.

As is clear from the variety and breadth of the standards, bodies, and organizations that industry relies on, many companies believe that a variety of standards and best practices contribute to supply chain integrity. But as discussed earlier, there is also compelling evidence that there are gaps and contradictions in the government's policies and practices that contribute to supply chain risk. Here are a couple of proposals that, if addressed, could have immediate impact on securing the communication supply chain. First, the Executive Branch, at the urging of this committee, of course, should issue a directive requiring federal departments and agencies to purchase only from trusted and authorized sources, especially for mission-essential functions, unless there is some compelling reason to go outside of that channel. If there is such a compelling reason, the purchaser should be required to put a justification and authorization in writing. It is low-hanging fruit; we should do it immediately.

Second, the government should require that small business vendors be certified as authorized resellers and partners. Requirements pertaining to small business set-asides also have the secondary impact of causing procurement officers to pursue acquisitions through providers who are not part of the authorized and trusted supply chain.

We all understand the importance of small businesses to the government's industrial base and to the economy in general. It is important to recognize that bad actors also exploit our reliance on small business as a means of entry. Counterfeiters and others attempt to introduce their tainted equipment into our critical infrastructure through small business enterprises.

Third, members of this committee have been involved in attempting to pursue better information-sharing. We support CISPA and we appreciate all the good work here and hope that you will support moving that bill through the Senate.

While we are working on legislation to break down barriers to improve timely, reliable, and actionable situation awareness, there is a step we could take immediately. We continue to hear that the government has significant concerns about supply chain and the threat to national and economic security. The government has access to case studies of successful, unsuccessful, interrupted, or disrupted attempts to perpetrate network intrusions through the supply chain. We should take those lessons learned from those experiences and share the tactics, techniques, and procedures, not sources and methods that cross over into the classified space that we can learn from and better inform the community in their own risk management decision-making.

There are a couple of others in my testimony I hope that we will get to in the questions. But on behalf of the 9,000 proud employees of Juniper Networks, I thank you again for the opportunity to participate in this important discussion. Industry looks forward to continuing the collaborative relationship with Congress and the Administration on this important issue. I welcome your questions.

[The prepared statement of Mr. Dix follows:]

JUNIPER NETWORKS

"CYBERSECURITY: AN EXAMINATION OF THE COMMUNICATIONS SUPPLY CHAIN"

Statement of Robert B. Dix, Jr.
Vice President, Government Affairs and Critical Infrastructure Protection

before the

Subcommittee on Communications and Technology
Committee on Energy and Commerce
U.S. House of Representatives

Tuesday, May 21, 2013

EXECUTIVE SUMMARY

The Challenge

The government views its commercial supply chain as a major element in its risk profile, but many of its risk management efforts are not coordinated and were not developed in collaboration with industry even though industry also is concerned about supply chain security.

The government continues to make purchases from untrusted and unauthorized sources. The incentive to save money pushes agencies to brokers and other gray market suppliers that are not part of the authorized or trusted supply chain for original equipment manufacturers (OEM). This also is an area where much mischief takes place from both counterfeiters and those attempting to penetrate the government supply chain with malicious equipment.

When the government purchases equipment from unauthorized sources and then identifies it as counterfeit, it often assumes the OEM had a gap in its supply chain. The government does not instead ask why it bought sensitive ICT products from an untrusted source.

Industry Initiatives

While Juniper understands the importance of improving supply chain assurance for the Federal government, it often appears that the government does not understand the enormous investment that many in the private sector make to protect the integrity of their supply chain.

Juniper Networks has a supply chain assurance and brand integrity program for securing our products and supply chain. We employ best practices for supply chain security from organizations regarding component integrity; traceability of products; anti-counterfeit features; supplier selection; physical security; information and IP security; and channel monitoring and incident response. Finally, we work with industry partners and the government to identify emerging risks and on best practices to mitigate those risks.

Recommendations

1. The Government Should Purchase from Authorized and Trusted Sources
2. The Government Should Require that Small Business Vendors be Certified as Authorized Resellers and Partners
3. Enact Information Sharing Legislation as a Means toward Situational Awareness
4. Share Information about Tactics, Techniques, and Procedures More Broadly
5. Establish Incentives for Businesses to Certify their Security Practices
6. Education and Awareness Campaign

Good afternoon Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee. Thank you for inviting me to be a participant in today's hearing on the cybersecurity of the communications supply chain.

Background

My name is Bob Dix, and I serve as Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks. Juniper Networks is a publicly-held private corporation headquartered in Sunnyvale, California, with offices and operations around the world. We deliver trusted, high-performance networking and security solutions that help public sector agencies (spanning civilian, defense, and intelligence functions), private enterprises, and service providers deploy networks that are open, scalable, simple, secure, and automated. Juniper's portfolio includes software and systems for routing, switching, and security.

The Challenge

The government views its commercial supply chain as a significant element in its overall security risk profile; as a result, there are more than 100 different supply chain risk management efforts across the United States Government. Unfortunately, many of those efforts are not coordinated and were not developed in collaboration with private industry despite the fact that industry also is concerned about supply chain assurance (please see Attachment A).

I will address three aspects of this important subject of cybersecurity in the communications supply chain: first, the risk created by government procurement practices utilizing unauthorized equipment providers; second, supply chain integrity initiatives by industry generally, and

Juniper specifically; and third, several recommendations where the government can improve both government and private sector supply chain integrity.

Risky Procurement Practices

While industry is confronted with the challenge of monitoring and engaging with more than 100 different government supply chain risk management efforts, the Federal government itself continues to make purchases from untrusted and unauthorized sources on a routine basis. There was a well-publicized presentation in 2008 in which the FBI acknowledged that government agencies purchased networking equipment that was determined to be counterfeit through an online broker. This happens far too often, and we all know why this happens – it is about saving dollars.

There is an on-going culture across the Federal government, particularly at the program and project manager level, to be driven by cost and schedule. This is not malicious; it is just the way things have been for a long time. Many of our talented civil servants have their individual performance evaluations based on their ability to deliver projects and meet cost and schedule. This will often drive them to shop online to save dollars on a particular project. More often than not, this pushes them to brokers and other gray market suppliers that are not part of the authorized or trusted supply chain for original equipment manufacturers (OEM). This also is an area where much mischief takes place from both counterfeiters and those attempting to penetrate the supply chain with tainted or malicious equipment. Counterfeiters know the government's acquisition practices and use it to their advantage – they set up small gray market entities to sell equipment cheaply and online. This situation could get worse given the current budget climate.

Interestingly, when the government purchases equipment and then identifies it as counterfeit, it often assumes the OEM had a gap in its supply chain - pointing fingers at the private sector when, in many cases, they need to be looking in the mirror. The government does not instead ask why it bought a sensitive piece of IT hardware from an untrusted source. Here are a few real world examples:

- In April 2013, a Federal civilian agency issued a solicitation for maintenance of its Juniper Networks equipment. The Statement of Work that the Bureau issued with the solicitation states "Support has to be from Juniper directly or a Juniper approved support partner. This allows for diagnostics in order to determine the problem areas of the equipment and fast replacements of any parts that might fail." Approximately one week after the solicitation and Statement of Work issued, the agency awarded the contract to a company that is not an authorized support partner of Juniper.
- In July 2012, a defense agency purchased what it thought were new Juniper router interface cards from Unauthorized Reseller A. When the agency received the products, the boxes were open, ant-static bags were torn, and the products appeared to have been tampered with. The agency contacted Juniper, and our investigation revealed that Unauthorized Reseller A had purchased used Juniper equipment from a broker and sold it to the government as "new." It should be noted that the agency devoted significant resources to conducting a risk assessment with Juniper on the integrity of our products (presumably assuming that we were at fault), but this effort was rendered superfluous once it was determined that the agency had procured interface cards from an unauthorized entity.

- In October 2011, one of the military departments awarded a purchase order to Unauthorized Reseller S for Juniper Networks products. We contacted the military department and advised them that Unauthorized Reseller S was not authorized by us, but the buyer wanted to continue with the purchase because Unauthorized Reseller S was cheaper. In our investigation, we discovered that Unauthorized Reseller S was not a registered company; instead, it was a fictitious business name established by the individual owner of a previous business. The individual established the fictitious business name Unauthorized Reseller S following his 2011 release from prison for a conviction for trafficking in counterfeit network hardware. Once we provided this information to the military department, the department canceled the purchase order in favor of an authorized Juniper partner.

Industry Initiatives

While Juniper understands the importance of improving supply chain assurance for the Federal government, it often appears that the government does not understand the enormous investment that many in the private sector make to protect the integrity of their supply chain from concept to delivery. It is important to the business interests and brand reputation of Juniper Networks and other vendors and providers to maintain a productive and robust approach to supply chain security.

In fact, corporate supply chain integrity and assurance programs evolved at a very early stage in the technology sector, starting with the semiconductor industry in the early to mid 1980s when outsourcing of semiconductor packaging and assembly began occurring in many countries in Asia. These efforts continue and have been expanded partly due to high levels of chip theft in the semiconductor transport industry and high levels of substandard product remarking, reselling, and gray marketing (please see Attachment B for a more comprehensive list of such efforts).

At a very early stage in our history, Juniper Networks established a formal supply chain assurance and brand integrity program for securing our products and our supply chain. The Juniper brand integrity program is one component of a comprehensive corporate security plan. At Juniper, we believe brand protection programs are inherently reactive to problems discovered in the channels. Juniper's philosophy has been to implement security and integrity best practices throughout our product lifecycle process to prevent instances of counterfeit products or components, and to ensure that our customers receive the highest quality products available in the marketplace.

Juniper references numerous international standards in the operation of its supply chain and brand integrity programs, including:

- ISO 27001 for information security
- ISO 9001 / TL9000 Quality management system (Certified)
- C-TPAT and AEO supply chain security criteria (Certified Tier 3 C-TPAT and AEO- Security)
- Common Criteria product certifications

We also employ best practices for supply chain security from organizations such as The Open Group Trusted Technology Forum (O-TTF); the Alliance for Gray Market and Counterfeit Abatement; and the Software Assurance Forum for Excellence in Code (SAFECode). Some of these best practices include: component integrity assurance; traceability of products and components; anti-counterfeit features within our products; supplier selection (including an evaluation of foreign interests, relationships, and potential for foreign control); physical security; information and IP security; and channel monitoring and incident response. Finally, we work with our industry partners and the government to identify new and emerging risks and collaborate on best practices to mitigate those risks.

Recommendations

As is clear from the variety and breadth of standards bodies and organizations that industry relies on, many companies believe that a variety of standards and best practices contribute to supply chain integrity; but, as discussed earlier, there also is compelling evidence that there are gaps and contradictions in the government's policy and practices that contribute to supply chain risk. Here are a few proposals that, if addressed, could have immediate impact on securing the communications supply chain:

1. <u>The Government Should Purchase from Authorized and Trusted Sources</u>

The Executive Branch should issue a directive requiring Federal departments and agencies to purchase only from trusted and authorized sources unless there is a compelling reason to go outside of that channel. If there is a compelling need to purchase from unauthorized vendors, such as for obsolete parts, the government should issue a written Justification & Authorization (J&A) and assume the liability of such a decision. In conjunction with this, acquisition officers should be evaluated based on their ability to procure goods and services that deliver the best value for the government over the long term instead of those that appear to be the lowest price in the short term; a product that is less expensive in the short term might end up costing more over the long term as a result of additional maintenance, more frequent replacement, higher energy costs, etc. Together, these reforms would mitigate a significant amount of the government's supply chain risk.

2. The Government Should Require that Small Business Vendors be Certified as Authorized Resellers and Partners

Requirements pertaining to small business set-asides also have the secondary impact of causing procurement officers to pursue acquisitions through gray market providers who often are not part of the authorized and trusted supply chain; gray marketers set themselves up as small businesses. While Juniper Networks understands the importance of small businesses to the government's industrial base and to the economy in general, it is important to recognize that bad actors often exploit our reliance upon small business as a means of entry. Counterfeiters and others attempt to introduce their tainted equipment into our critical infrastructure through small business enterprises.

Companies like Juniper Networks welcome and value the opportunity to work with small businesses. We have programs that invite participation by small business providers to become part of the authorized and trusted network of resellers and partners. The government should require that all of its vendors, including small businesses, be authorized to resell the equipment they are providing.

3. Enact Information Sharing Legislation as a Means toward Situational Awareness

Many of the Members of this Committee have been involved in attempting to address the issue of facilitating the exchange of intelligence information and creating a true partnership between government and industry to build enhanced situational awareness to improve detection, prevention, and mitigation of cyber events that may become incidents of national consequence.

Though the private sector is doing work internally to address the threat, the government has an important opportunity to significantly increase its communication of threat indicators and intelligence to industry. Far too often, the government continues to compartmentalize and restrict access to relevant information. In order for private industry to be able to prevent and mitigate threats, industry must have access to the threat information that the government possesses.

With this in mind, legislation introduced by a Member of this Committee, Rep. Mike Rogers (R-MI), in his capacity as Chair of the Permanent Select Committee on Intelligence, H.R. 624, the "Cyber Intelligence Sharing and Protection Act of 2013," would amend the National Security Act to facilitate the sharing of cyber threat intelligence with eligible private sector entities. This legislation will add an arrow to the protection quiver by addressing a key impediment to building cyber situational awareness and passed the House on a wide bipartisan margin. Juniper Networks hopes that you will join with your Intelligence Committee colleagues in urging the Senate to take up this important bill.

4. Share Information about Tactics, Techniques, and Procedures More Broadly

While we are working on legislation to break down barriers to improving timely, reliable, and actionable situational awareness, there is a step we could take immediately. We continue to hear that the government has significant concerns about supply chain and the threat to national and economic security. The government has access to case studies of successful, unsuccessful, interrupted, or disrupted attempts to perpetrate network intrusions through the supply chain. We should take the lessons learned from those experiences, and share the tactics, techniques, and procedures (not sources and methods that cross over into the classified space) that we can learn from and better inform the community in their own risk management decision making.

5. Establish Incentives for Businesses to Certify their Security Practices

As part of its procurement evaluation process, the government should examine incentives that would provide recognition to companies that choose to have their security processes and practices certified and accredited by recognized standards bodies. Most businesses already manage their security risk but might not seek to have their practices certified because there is no customer incentive to do so. If a large buyer, like the government, were to recognize such certifications, more businesses would potentially be incentivized to apply for them.

6. Education and Awareness Campaign

As we are all aware, the inadvertent introduction by employees and contractors of malware is one of the primary sources of infection adversely impacting cybersecurity. The communications supply chain is no exception to this problem and a larger effort to combat this has benefits in and beyond supply chain integrity. The government should develop a coordinated and long-term education and awareness campaign for cybersecurity. When our Nation was confronted with the threat of the H1N1 virus, the government mobilized agencies and the private sector to advise individuals how to protect themselves from the risk of infection. There were public service announcements, posters, radio, TV, and Internet messages regarding the need to cough into our sleeves, wash our hands, and other protective measures to secure our health. The effort included the CDC, HHS, and other federal departments and agencies, along with many non-profits, businesses, and organizations.

We have the opportunity to use the same model for a sustained awareness program to help educate citizens, small businesses, students, non-profits, and other stakeholders on how to protect themselves from the risk of malware, phishing and other forms of infection in cyberspace.

Many Federal departments and agencies routinely interact with citizens and businesses. Leveraging the Small Business Administration; the Internal Revenue Service; the U.S. Postal Service; the U.S. Department of Education; and others would provide an ability to scale the messaging across a wide range of the population. Perhaps we could even convince every Member of Congress to include a link on their website that directs constituents to where they can get more information about protecting their health in cyberspace.

Conclusion

On behalf of the more than 9,000 proud employees of Juniper Networks, thank you again for this opportunity to participate in this important discussion. Industry looks forward to continuing the collaborative relationship with Congress and the Administration on this important issue.

APPENDIX A

1. In February 2013, the President issued a cybersecurity Executive Order.

2. Recently-enacted editions of the National Defense Authorization Act (NDAA) and the Intelligence Authorization Act contained provisions that provide the government with expanded authority to exclude private sector vendors from eligibility for Federal procurements based on a presumed national security risk without notice.

3. In 2011, the Department of Commerce, acting on behalf of the Department of Defense, distributed surveys to industry under the auspices of the Defense Production Act (DPA). The Defense Supply Chain Network survey (or sector-by-sector, tier-by-tier evaluation (S2T2)) asked for sensitive and proprietary company information and suggested the threat of jail time for failure to comply.

4. In 2011, the U.S. Intellectual Property Enforcement Coordinator issued a request for comments as part of an inter-agency effort to reduce counterfeit products from the U.S. Government supply chain.

5. In 2008, there was a Federal Acquisition Regulation proposal to impose unlimited liability against private sector providers if counterfeit equipment was found in the government's operation, even if that equipment was not from a manufacturing or assembly facility of the named provider.

6. Supply chain activities taking place pursuant to the Comprehensive National Cybersecurity Initiative (CNCI) #11 have not included private sector participation.

APPENDIX B

1. Transported Asset Protection Association (TAPA) (originally the Technology Asset Protection Association)

2. High-Tech Crime Investigators Association (HTCIA)

3. ASIS International

4. International Security Management Association (ISMA)

5. Coalition Against Counterfeit and Piracy (CACP)

6. CSO Roundtable

7. Internet Consortium for Advancement of Security on the Internet (ICASI)

8. Information Sharing and Analysis Centers (ISACs)

9. Sector Coordinating Councils (SCCs)

10. The Partnership for Critical Infrastructure Security (PCIS)

11. The President's National Security Telecommunications Advisory Committee (NSTAC) and National Infrastructure Advisory Council (NIAC)

Mr. WALDEN. Mr. Dix, thank you very much.

They have called the votes. I believe they have, right? And so we will recess at this point. So close, Mr. Rothenstein, so close. And then we will come back and start with you and get to our other two witnesses, and then Q&A. So thank you for your patience and we will be back shortly.

[Recess.]

Mr. LATTA [presiding]. I would like to call the subcommittee back to order. And I believe next in order of our witnesses is Mr. Rothenstein, and thanks very much for being here today. We appreciate your testimony.

STATEMENT OF DAVID ROTHENSTEIN

Mr. ROTHENSTEIN. My pleasure. I hope that delay only served to build anticipation of my testimony.

Vice Chairman Latta, Ranking Member Eshoo, members of the subcommittee, my name is David Rothenstein and it is my pleasure to appear before you today. I serve as senior vice president and general counsel of Ciena Corporation, a publicly held Maryland-based provider of equipment software and services that support transport and switching, aggregation management and voice, video, and data traffic on communications networks. Our products are used by communications network service providers, cable operators, governments, and enterprises across the globe.

Today, a number of current market trends, including the proliferation of smartphones, tablets, and mobile devices, are substantially increasing the demand on networks. This means that Ciena must deliver faster, more efficient, and more secure equipment to our customers to help them meet their end-user requirements.

As with most technology companies, our success is largely driven by our innovation. Our global patent portfolio is our lifeblood and it enables us to develop leading-edge solutions and get new products to market quickly. In order to support this continuous innovation and because our equipment sits in critical infrastructure networks around the world, Ciena's executive team spends a lot of time looking at the intersection of cyber security and supply chain.

Because our customers demand best-in-class product delivery lead times, quality and performance, security of supply, and product security and integrity, we have taken steps during the past few years to transform and optimize our supply chain operations. These changes have enabled us to use our supply chain as a differentiator in the market.

One example of these changes has been our focus in designing and manufacturing equipment and software that meets or exceeds the security needs of our customers. For years, our customers have generally inquired with us about the security, integrity, and assurance of their networks. With this in mind, in 2011 we performed a detailed analysis of our supply chain that considered a range of factors.

As a result of this analysis, we decided at that time to begin a gradual exit from China of key elements of our supply chain. This was not an easy decision. China represents one of the largest and fastest-growing markets for communications equipment in the world. And the country is home to the fabrication facilities that produce many of the components that go into our products. However, based on what we knew about our products, our customers, and the business and security environment in China, we decided to make this change.

In contrast to some of our peers, we weren't as concerned about the potential adverse impact of this decision on our sales opportunities in China. Several years ago, because of the significant barriers to entry and the technology transfer requirements to do business in China, we decided not to pursue a go-to-market sales strategy in that country. We are now almost 2 years into our supply chain transformation. By the end of 2013, we will have transitioned all of the manufacture and assembly of our products and a sizable portion of our global spend on finished and semi-finished assemblies from China to other jurisdictions, primarily Mexico and Thailand. In so doing, we have increased the velocity of our supply chain, solidified our security of supply, and insured the security and assuredness of our products. At the same time we have remained very competitive in the market from a cost standpoint.

There are some parts that we continue to source from China. We are in active discussions with our major vendors as to their plans for transitioning out of China, largely to address issues relating to counterfeit goods and intellectual property infringement. We are less concerned about the security vulnerabilities of these products even if they are primarily passive products that are neither programmable nor capable of being embedded with damaging computer code or malware.

At the same time, we have taken extensive steps to ensure the integrity of the active or programmable components in our products. We require now that these components are sourced from outside of China. We maintain rigorous and internal practices and capabilities that enable us to identify any issues with respect to the security of our components. And by implementing strict controls over our own software developments and by ourselves performing the final testing and validation of the software loaded on to our products, we ensure the integrity of our software, which is the critical element that controls and manages our products and our customer's networks.

In conclusion, Ciena applauds the Subcommittee for taking on this issue. In our case, we proactively elected to make changes to our supply chain and not to wait for legislation, regulation, or the Administration's implementation of the recent Executive Order on cyber security. Instead, we talked to our customers, conducted a thorough business analysis and risk assessment, and made a decision that we continue to implement today. While this strategy may not necessarily work for others, it has worked effectively for us. It makes good business sense and delivers additional security for our customers and for their networks.

With that, I conclude my remarks and am pleased to take any questions.

[The prepared statement of Mr. Rothenstein follows:]

Written Statement of
David M. Rothenstein
Senior Vice President, General Counsel and Secretary
Ciena Corporation

Before the Subcommittee on Communications and Technology
House Committee on Energy and Commerce
Hearing on "Cyber security: An Examination of the Communications Supply Chain"

Introduction

Chairman Walden, Ranking Member Eshoo, Members of the Committee, my name is David Rothenstein and it is my pleasure to appear before the Subcommittee this afternoon examining the intersection of cyber security and the supply chains of companies who operate and who supply equipment for communications networks.

Company Background

I serve as Senior Vice President, General Counsel and Secretary of Ciena Corporation, a Hanover, Maryland, based global provider of equipment, software and services that support the transport, switching, aggregation and management of voice, video and data traffic on communications networks. Our Packet-Optical Transport, Packet-Optical Switching and Carrier Ethernet Solutions products are used in communications networks operated by service providers such as AT&T, CenturyLink, Verizon, BT (also known as British Telecom), SingTel (Singapore's telecommunications company) and Telefonica Vivo (the largest mobile operator in Brazil); by cable operators such as Comcast and Rogers; and by research and education institutions, enterprises and other network operators around the globe.

In addition to ongoing projects with the world's largest service providers, some recent examples of our work include:

- provision of converged packet-optical and packet networking solutions to Integra, a provider of fiber-based, carrier-grade networking solutions based in Portland, Oregon, for the expansion of its long-haul fiber optic network; and
- an award to power the Illinois iFiber optical network, which is designed to service small business, local governments and universities in northwestern Illinois.

In addition, through our government solutions subsidiary, Ciena is a direct and indirect supplier of networking equipment, software and services for some of the United States' most critical government infrastructure projects. Since 2004, Ciena has provided the optical transport equipment for the U.S. Department of Defense's Global Information Grid Bandwidth Expansion (GIG-BE) Program, a net-centric transformational initiative to provide high-speed communications capability to key operating locations worldwide. In 2011, Ciena partnered with Internet2, a non-profit community of universities, companies, government agencies and others, on a 100G national network in support of the U.S. Unified Community Anchor Network (U.S. UCAN) project. And, Ciena has built assured, adaptive optical networks for a number of U.S. armed services base infrastructure projects and provided managed services for the networks of several U.S. government agencies and various state and local governments.

Ciena was founded in 1992 with the desire to radically change the possibilities and economics of networking. Over 20 years later, we have accomplished that objective, becoming an innovator in delivering solutions that enable converged, next-generation architectures around the world. Today, a number of market trends – including the proliferation of smartphones, tablets and similar devices running mobile web applications; the prevalence of video applications; and the shift of enterprise and consumer applications to cloud-based or virtualized network environments – are indicative of increasing use and dependence by consumers and enterprises on a growing variety of broadband applications and services.

This significant increase in multiservice network traffic will require network operators to invest in next-generation, high-capacity network infrastructures that are more robust and efficient. Accordingly, Ciena's network architecture vision and approach, which underpins our solutions offerings and guides our research and development strategy, leverages the convergence of optical and packet networking technologies to increase network scale cost effectively, while emphasizing software-enabled programmability, automation and open interfaces. Through this network approach, we enable high-capacity, configurable infrastructures that can be managed and adapted by network-level applications to create new communications services, and that provide flexible interfaces for the integration of computing, storage and network resources. By increasing network flexibility for service delivery, reducing required network elements and enabling increased scale at reduced cost, our communications networking solutions create business and operational value for our customers. Simply put, our equipment, and that of our peer vendors, makes up the backbone of the global communications infrastructure. And we are enabling more people to use it with more devices at higher speeds, and more reliably, than ever before.

Our success is driven by our innovation. Years of creating solutions for the world's largest and most reliable communications networks have led to more than 1,550 U.S. patents and patent applications, as well as more than 500 foreign-issued patents and patent applications. Like many technology companies, patents are our life blood, and enable us to innovate quickly and get new products into the global market.

Cyber Security and Supply Chain

In order to support this continuous innovation, and because our equipment serves as the core of communications networks around the world, Ciena's executive leadership team spends a lot of time looking at the issue before the subcommittee today – the intersection of cyber security and supply chain. It is a topic on the minds of all of our existing and prospective customers, particularly the service providers, and we aggressively seek their input and perspectives in order to learn what they value in their suppliers and in their networking equipment.

The stated goal of our supply chain operations team is to implement a "value driven" supply chain, one which drives changes that will create value for Ciena and for our customers. A key aspect of the success of such a model is the ability to manage the inherent complexity of the supply chain while ensuring a positive and differentiated customer experience. We have heard from our customers, and they clearly value things like performance against shorter product delivery lead times, outstanding product quality and performance, security of supply, and product security and reliability.

Based on that feedback, we have undertaken a number of actions to transform and optimize our supply chain over the past few years. These actions were taken from both a business and a security perspective, as we operate in a very competitive global marketplace with competitors many times our size.

One way we use our supply chain to differentiate ourselves from our peers is by trying to be faster to market. For example, we implemented a "direct order fulfillment" (DOF) model for several of our products. Under this model, we select contract manufacturers whose facilities are located closest to our primary North America market and require the manufacturers to perform final assembly and testing of our products and to ship the products directly to our customers. By eliminating a key step in the process, the DOF model allows us to improve our supply chain velocity and ensure performance to stated product delivery lead times in a very cost-efficient manner. Similarly, we consolidated our global logistics partners to ensure a simpler model that is geographically closer to our primary market and has cleaner and more optimized shipping lanes.

In addition to assessing our overall supply chain with the goal of improving velocity and cost, we also focused on how best to design, build and manufacture equipment and software that meets or exceeds the security and reliability needs of our customers. Given all of the news of cyber security intrusions, vulnerabilities, intellectual property infringement, data exfiltrations and the like, many parts of our customer base have been aware of the issue for some time and continually press us on issues relating to product security, integrity and assurance.

I am sure that the Members of this committee are well aware of the increasing prevalence and severity of cyber threats directed against our government and U.S.-based defense contractors, critical infrastructure owners and operators, and high technology companies, including those threats that emerge every day from China. Our government and several private sector organizations, including security firm Mandiant, have documented this very well, and it is not necessary to belabor the point. Suffice it to say that as a company selling equipment and software that sits in the core of critical communications network infrastructure, we began to question the level of supply chain exposure to the design and manufacture of key products originating in China.

With all of this in mind, we undertook a comprehensive analysis of our supply chain and considered a range of issues, including:

- the amount of the supply chain originating in China as compared to other countries around the world;
- the portions of our products that we considered to be particularly vulnerable from a security standpoint;
- the alternate sources of supply for those products, both in terms of companies and geographies;
- proximity to our key North America market;
- the cost impact of any transition, including labor and overhead costs;
- the relative political and social stability of various locations; and
- the potential impact of any transition upon product test capacity, lead times, quality or performance.

As a result of this analysis, in the middle of 2011 we made a conscious decision to begin a gradual exit of key elements of our supply chain from China. At the time, over one-fifth of our global supply chain spend on contract manufacturers originated in China, and approximately two-thirds of our global spend on finished and semi-finished assemblies originated from the China-based facilities of original equipment manufacturers.

Obviously, this was not an easy decision. China represents one of the largest and fastest growing markets for communications networking equipment in the world. And, with a very low cost manufacturing base, China is also home to the manufacturing facilities that produce many of the components and subcomponents that go into our products. However, based on what we knew about our products, our customers and the overall business and security environment in China, we decided to make this change.

In making this decision, and in contrast to some of our peers, we were not as concerned about the potential impact on our sales opportunities in China. Several years ago, we made the deliberate decision not to pursue a go-to-market sales strategy in China. Because well over 90% of networking equipment sales into the China market is controlled by Chinese equipment vendors, and because of domestic production requirements that require the transfer of intellectual property that we were not willing to entertain, we determined that the barriers to entry into the China market were too high to pursue meaningful sales opportunities in that country.

We are now two years into this aspect of our supply chain transformation. During this time, we have made substantial progress toward our goal of increasing the velocity of our supply chain and the security and assuredness of our products. By the end of 2013, we will have effectively moved all of the manufacture and assembly of our products out of China, and we will have reduced our global spend on finished and semi-finished product assemblies originating from China to less than one-half. We have effectively transitioned these elements of our supply chain to other jurisdictions – primarily Mexico and Thailand – that offer a combination of increased time-to-market, improved security of supply, and increased product security and reliability. For example, with approximately 85% of our global contract manufacturer spend now based in Mexico, we have decreased our product lead times, with the products being driven by truck across the U.S. border as opposed to being sourced from China and then sent via maritime container ship to the U.S. At the same time, by partnering effectively with our contract manufacturers and aggressively pursuing cost reductions though lower labor and landed cost rates, we have not incurred a significant increase in the cost of our products. We have remained competitive in the market from the standpoints of technology, delivery and cost, and we continue to win business from existing and new customers and take market share.

With respect to those finished or semi-finished assemblies that remain sourced from China today, we are in active discussions with our major vendors as to their plans for transitioning out of China. As a result, we expect the overall percentage of products originating from China to continue to decrease over time.

We remain focused on this effort primarily to reduce the risk of intellectual property infringement and the incorporation of counterfeit components into our products. Until then, we believe that continuing to source several specific products from China presents low risk from a security, integrity and reliability standpoint. These finished and semi-finished assemblies, such as optical passive modules, power rectifiers and mechanical assemblies, are largely "passive" products in that they are neither programmable nor capable of being embedded with damaging computer code or malware. In an abundance of caution, though, we perform system field tests on most of these products prior to deployment.

Similarly, there remain certain parts used in our products – such as capacitors (which are used to store energy), heat sinks (which cool electronic devices) and filters, often collectively referred to in the industry as "jellybean" or "peanut" parts – for which we have not attempted to transition the supply chain out of China. Because the source of supply for these parts is limited only to manufacturing facilities in China, we expect to continue procuring them from China. However, as these parts are incidental to the actual functionality of the products and are neither programmable nor susceptible to being compromised in any way from a security standpoint, we are confident that they present very limited risk to the overall integrity and security of our products.

Separately, we have taken extensive steps to ensure the security and reliability of the "active" components in our products, such as programmable logic integrated circuits, analog integrated circuits, digital signal processors, field-programmable gate arrays and microprocessor integrated circuits. First, we ensure that all of these components are sourced from outside of China. For example, the key active components in WaveLogic 3, our industry-leading 100G coherent optical chipset, were designed and developed in North America and Europe. Second, we provide an approved vendor list to our contract manufacturers, who then procure these products and incorporate them into the assembly of our products. Third, we maintain rigorous internal practices and capabilities that enable us to identify any discrepancies in the performance, behavior and security of these component assemblies. And fourth, by implementing strict controls over our software development, and by performing the final testing and validation of the software loaded onto our products, we ensure the integrity and reliability of the critical element – software – that controls and manages our products and our customers' networks.

In taking these steps, we believe not only that our company has become more efficient and able to deliver products more quickly but also that our customers are getting more secure and trusted products. Indeed, we have received extremely positive feedback from many of our service provider and government customers in response to this element of our supply chain transformation. In sum, while we recognize that this supply chain strategy may not necessarily make sense for all other companies, it has worked quite effectively for Ciena and our customers.

It is fair to say, however, that many potential purchasers of networking equipment, software and services – particularly enterprises that buy equipment for their own networks – still do not appreciate the cyber security threats facing our nation today. That is why Ciena was pleased to support the Cyber Intelligence Sharing and Protection Act, HR 624, authored by committee member and House Permanent

Select Committee on Intelligence Chairman Mike Rogers, and Ranking Member Dutch Ruppersberger. We believe that broader sharing of cyber threat information would be particularly valuable for the many private sector companies, particularly those in the critical infrastructure area, who demand trusted and secure networks but do not have access to the same level of information and resources as the largest communications service providers and governments.

Conclusion

In conclusion, Ciena applauds the subcommittee for taking on this issue of cyber security and the communications supply chain. As you now know, Ciena elected not to wait for legislation, regulation, or implementation of the Obama Administration's Executive Order on cyber security, to make changes in its supply chain. Instead, we talked to our customers, conducted a thorough business analysis and risk assessment, and made a decision that has been and is continuing to be implemented today. We are confident that taking these steps makes good business sense for our company and delivers additional security for our customers and their networks.

Mr. LATTA. Well, thank you for your testimony.

And our next witness is Mr. John Lindquist, President and CEO of EWA Information and Infrastructure Technologies, Inc. Good afternoon and thanks for testifying.

STATEMENT OF JOHN LINDQUIST

Mr. LINDQUIST. Thank you, Mr. Vice Chairman, members of the committee. Thank you very much for the opportunity to testify.

As we all know, the security of our telecom systems is in fact very critical. We are aware of the myriad threats to the U.S. and the threat is real but is not limited to a single country, geographic area, or organization. Protection is made difficult because the supply chain for electronic systems and devices in general and specifically telecommunication systems is truly global. Most of the telecom system vendors have very large footprints in China and elsewhere around the globe, and many of these worldwide locations are easily and directly accessible by the various threat nations and organizations.

Furthermore, it is the nature of the system development to make use of software routines and hardware components that are generally available in the market, and it is virtually impossible to determine the pedigree of all of the hardware and the software that goes into a telecommunications system. Our adversaries are professional, highly technically capable intelligence organizations or sophisticated criminals, neither of which would have any difficulty circumventing a trusted supplier system.

To address the security dilemma effectively, an evidence-based security process should be applied, that enables an informed judgment that an adequate level of assurance has been provided that the system is free of malicious features and does not contain serious security defects; and that is without regard to origin of the system.

IIT had been selected by several telecommunications carriers as an independent evaluator to implement such a process. The process we are implementing is comprised of two major phases. The first is an in-depth security assessment of the system software, hardware, and firmware to include all patches, upgrades, and modifications as they occur.

The second phase is a delivery process that ensures that the deployed system and all patches, upgrades, and modifications are exactly the ones that were evaluated and determined to be suitable and acceptable. The key features of the process include: willing participation of the developer and vendor; a trusted independent evaluator; direct coordination between and among the stakeholders, particularly the telecoms and the concerned government agencies and the evaluator without interference or necessarily knowledge of the vendor; correction of unintentional defects before deployment; immediate involvement of law enforcement if evidence of malicious intent is discovered; and a delivery system that ensures that the system delivered matches the evaluated system and prevents the vendor or any other un-presented party from accessing the system during or after delivery; and finally, a scheme for monitoring the system after deployment.

In our case, the vendors have been very willing to comply because compliance was a condition of the sale to the telecommunications carrier. Under those contracts, they provide us the design documentation, source code, the complete set of sample components, replication of the compilation environment for their software and firmware, advance notice of all design changes, patches, and modifications, and access to their development facilities to provide us the understanding of their process.

We were selected because of our intimate knowledge of the threat. We have a comprehensive process with clear analytical and reporting criteria that explicitly addresses the evolving threat. We have secure facilities. We use exclusively U.S. personnel, who have been vetted through the U.S. security clearance process, and we have a staff fully qualified and equipped to perform the evaluations.

The contracts in each case specifically provide for the direct private communication between the evaluator and stakeholders. Telecommunication carriers, by contractual mandate, are the primary beneficiary of our work. A condition of acceptance is a report from us describing what we did, the faults found, the correction implemented, and any residual risk, and we are free to discuss any issues directly with the telecom and the government.

In our lab, we subject the system to a detailed analysis, both a static analysis of the software and a dynamic testing of the software and hardware. There have been thousands of defects found and mitigated, not all of these in Chinese systems; as a matter fact, many of them in systems that currently exist in the telecommunication system.

The software is delivered directly from us to the networks. The hardware is subjected to a random sampling process, and the firmware is either delivered directly from us or the boards are reflashed by us, all again to make sure that the delivered software is what we evaluated. Our recommendation is that some evidence-based security process like this is included in the government's approaches, including the NIST security framework and other programs across the government.

Thank you very much.

[The prepared statement of Mr. Lindquist follows:]

Testimony before the Subcommittee on Communications and Technology
Date of Hearing: 21 May 2013
Witness: John W. Lindquist
President & CEO
EWA Information and Infrastructure Technologies, Inc
CEO
EWA North America, LLC

Mr. Chairman and Members of the Committee,

Thank you for the opportunity to testify on the very important issue of the Security of the Communications Supply Chain.
My expertise and that of IIT, the Company I represent, within the overall process of Supply Chain Security is security suitability and acceptability.

The security of our telecom systems is critical. We are all very aware of the myriad number of threats from nations and organizations unfriendly to the U.S. I leave it to the U.S. Intelligence Community to to characterize that threat but I have sufficient insight to be convinced that the threat is very real, is not limited to a single country, geographic area or organization, and that we must protect ourselves..

That protection is made more difficult because the supply chain for electronic systems and devices in general and specifically telecommunications systems is truly global. There are no manufacturers of telecommunications systems in the U.S. Two of the major telecom system vendors are Chinese, and the other three are European and, those European vendors have very large footprints in China and elsewhere around the globe. Many of these worldwide locations are easily and directly accessible by the various threat nations and organizations. Furthermore, it is the nature of system development to make use of software routines and hardware components that are generally available in the market. It is virtually impossible to determine the pedigree of all of the hardware and software that goes into a telecommunications system. Further, it is not practical to impose a system of trusted suppliers for all of the components. Such a system would be virtually impossible to police and self certification of processes is of little to no value. Our adversaries are professional, highly technically capable, intelligence organizations and/or sophisticated criminals, neither of which would have any difficulty circumventing a self certification system. The bottom line is that the embargo of products from certain countries or companies does not provide secure systems.

To address this security dilemma effectively an Evidence Based System Process (EBSP) must be applied that enables informed decisions as to the security suitability and acceptability of a system before it is deployed and throughout its life cycle.
To be suitable and acceptable, there must be reasonable assurance that any system being introduced into our telecommunications networks are free of malicious features and serious security related defects. It is very likely that the legacy systems, those already in operation, are not free of such security defects and it is unknown if malicious capability has been introduced into the systems. However, it is not practical to shut down our networks to assess the current systems. Thus, the focus must be on new systems and system upgrades. The analytical results on new systems provide insight into the nature of probable security relevant defects in the legacy systems which can be addressed through network security techniques, most likely increased effective monitoring.

The EBSP should be comprised of two major phases. The first is an in depth security assessment of the system to include all patches, upgrades, and modifications as they occur, and the second being a delivery process that insures that the deployed system and all patches, upgrades, and modifications are exactly the ones that were evaluated and determined to be suitable and acceptable.

The key features of the EBSP are:

- Willing participation of the developer/vendor.
- A trusted independent evaluator.
- Direct coordination between the stake holders,(telecoms and concerned government agencies) and the evaluator without interference or knowledge of the vendor.
- Correction of unintentional defects before deployment.
- Immediate involvement of law enforcement if evidence of malicious intent is discovered.
- A delivery system that insures the delivered system matches the evaluated system and prevents the vendor or any other un-trusted party from accessing the system during or after delivery.
- A scheme for monitoring the system after deployment.

We have implemented an EBSP that includes the above features with several telecommunications companies here in the US and Canada performing evaluations and deliveries of multiple vendors products which are being integrated into a LTE upgrade. The results of the evaluations, although not completed, have yielded significant security benefit to the recipient. As a result of our analysis, an extremely large number of security relevant defects have been identified and corrected or are in the process of being corrected. Although we have found no evidence of malicious intent, we have caused the elimination of serious vulnerabilities that the threat would have been able to exploit. These serious defects were found equally in Chinese and non-Chinese vendors products.

In our EBSP, the Vendors have been very willing to comply because their participation in the EBSP was a condition of the sale to the telecommunications company.

The vendors have provided:

- Design documentation for hardware, software, and firmware.
- Source code for system software and firmware.
- A complete set of sample components.
- A replication of the compilation environment for their system.
- Advance notice of all design changes, patches, and modifications with subsequent delivery to us of the changed product.
- Access to their development facilities to provide us understanding of their development process.

We have been selected by the vendor and the telecom carrier as the trusted independent evaluator based on their evaluation of the efficacy of our process and the trustworthiness and qualifications of our personnel. Specific criteria used were:

- A comprehensive process with clear analytical and reporting criteria.
- Secure laboratory facilities suitable to protect the intellectual property of the vendor.Our facility is designed to Sensitive Compartmented Intelligence Facility specifications.
- The use of exclusively US personnel with Top Secret security clearances. Although the work is not classified, the use of cleared personnel assures that they have been fully vetted and found to be trustworthy.
- A staff fully qualified and equipped to perform the evaluations and effect trusted delivery.
- We are paid by the telecommunications company not the vendor.

The contracts in each case specifically provide for the direct, private communication between the evaluator and the stakeholders.

- The telecommunications carrier is, by contractual mandate, the primary benficiary of our work
- A condition of acceptance of the product is a report from us describing faults found, correction implemented and any residual risk.

- The evaluator may discuss any issues directly with the telecom and/or government agencies without notifying the vendor or providing the vendor the outcome of any such discussions.

In our labs, we subject the system to a detailed evaluation. The evaluation is designed to identify the existence of paths through which all known threats could compromise the system. The evaluation includes:

- Static and dynamic evaluation of the source code and software binaries.
- Evaluation of the vendor compilation environment and compilation scripts.
- Evaluation of the hardware components at the board and chip level. Hardware is evaluated to the level of detailed printed circuit board layout, discrete components and signal paths in and among circuit boards. Hardware is also characterized to the board and key component level, to enable the trusted delivery verification process. Dynamic testing of the system.

There have been thousands of defects found. In each case the vendor has been asked to explain the design purpose or other reason the condition exists, to include programmer error and to provide their intended fix. In this exchange, the vendor is not provided with a description of the specific test methodology applied by the evaluator, nor any unique information regarding what we might know about the relevant threat or how the vulnerability might be exploited. The vendor's response in consideration of the seriousness of the defect are used to make an evaluation of intent as malicious or not malicious. There have been no findings of malicious intent thus far. If there had been it would have been reported directly to the FBI. Once the fix is negotiated as adequate, the modified code is again subjected to a complete evaluation to insure that the defect was properly corrected and that no other defects were introduced.

Of significance is the value added operational benefits that accrue through this process. Operational efficiencies increase speed, agility, and baseline system performance. We produce for both the vendors and the telecommunication providers a system that has been rigorously tested and enhanced.

Once the system is deemed security suitable and acceptable for deployment by the telecommunications company we implement a trusted delivery process which includes the delivery of the software, firmware and hardware.

- The software is delivered directly from us to the telecommunications carrier via a secure network connection. Prior to delivery, it is compared against a record set of binaries compiled independently by us using evaluated source code. If the two software binaries match, the software is transmitted to the carrier. If problems are detected, the issues are resolved prior to delivery of the software to the carrier.

- The firm ware is generally delivered in a manner similar to the operating software, though it is often addressed through direct re-flashing of the boards by us after the devices have been delivered to the carrier or their trusted logistics provider.
- The hardware is subjected to a process of statistical sampling after delivery to the telecommunications company. The sample size is determined by the level of assurance required by the telecom. The telecom is then responsible for insuring the sample taken is truly random. A separate sample is taken for each shipment and each lot within a shipment. If upon comparison to the archived known evaluated board images. Ifa difference is found, the shipment is rejected.

Although none of the evaluated systems have yet been deployed, provisions have been made to conduct monitoring of special aspects of the system once it is running. This monitoring will be based on:

- Maintenance activities that despite all care might enable the introduction of malicious capability.
- Random scientifically based sampling to manage residual risks.
- Indications of specific activity either through normal monitoring or communication with government intelligence activities advising of additional threats and threat intent.

To date our EBSP has provided the ability to significantly improve the security posture of the affected telecommunications company at a very reasonable cost, when considered as a percent of the total cost of the system. The cost is down significantly after the initial evaluation. Costs are further mitigated by the improved performance of the system stemming from the removal of identified defects, security related or not.

By providing the recipient telecommunications company with the evidence to make an informed security decision, they are able to procure the best systems and benefit from a truly open competitive market environment.

I strongly recommend that the Evidence Based Security Process (ESBP) approach be integrated throughout the NIST Security Framework and other security policy and process initiatives across the government. Although not part of this discussion, it is a fact that our eighteen critical infrastructures rely on System Control and Data Acquisition (SCADA) systems as well as Industrial Control Systems(ICS) in which lack required levels of security. The broad use of independent and comprehensive evaluations of critical systems is the best opportunity to improve security at an affordable cost.

Mr. LATTA. And thank you very much for your testimony.

Our next witness will be Dean Garfield, President and CEO, Information Technology Industry Council. And Mr. Garfield, you are recognized for 5 minutes.

STATEMENT OF DEAN GARFIELD

Mr. GARFIELD. Thank you, Mr. Chairman, since I see him walking back in, Mr. Vice Chairman, and Ranking Member Eshoo. On behalf of the world's most dynamic and innovative companies, I would like to thank you for all that this subcommittee and committee does on the issues that are most important to us and for spotlighting this issue today.

Supply chain integrity and assurance is core to who we are and what we do. It is a business imperative. And so we are encouraged to see the formation of a bipartisan working group and look forward to working with you. Your first principle, which is do no harm, is a good credo for all of the work that we do in this area.

I submitted testimony for the record and so I will focus my oral testimony today on three areas: one, providing a window into our supply chains; two is sharing some of the things we do both as individual companies and as a sector to ensure supply chain integrity; and then, third, to make some recommendations where Congress can be helpful.

I have the privilege of working for companies that are truly transforming the world. The products and mobile devices that we all walk around with every day are more powerful today than ever before. In fact, the mobile device that we all carry around has more processing power than the Apollo 11, or even more recently, the Mars rover. Those mobile devices are presented under a singular brand but they include hundreds, and in some cases, thousands of components.

To ensure that we are providing our consumers with the best products at the best prices, those components are sourced in the United States and in fact around the world as well to ensure that the services and the products that we deliver are consistently of the highest quality and that our global supply chains are highly integrated.

With that in mind, any change, risk mitigation, or otherwise around supply chain assurance is carefully calibrated and we would highly encourage that any advocacy or policy advance in this area be carefully calibrated as well.

The industry engages—both as individual companies and as well as a sector—in a number of steps to both manage and mitigate risk. As individual companies, they adopt and integrate best practices on a continuous and systemic basis that includes instilling and teaching secure sourcing, instilling and teaching secure coding, instilling and teaching identification authentication among a host of steps that are taken, some of which have been talked about by the other panelists generally.

As well, those individual steps that are taken by specific companies are complemented by industry-wide, sector-wide activities both through standards activities, and also through consensus-based voluntary global standard-setting organizations, such as ISO and IEC, which have advanced a number of standards that are quite relevant in this area, including the common criteria which is focused on product assurance or through standards that are focused on not products but the processes as well that complement those products, including the Open Group Trusted Technology Forum.

It is important to note that in both instances our government and other governments have an important role to play and do engage in those consensus-based voluntary global standards-setting organizations. In fact, over 26 countries have adopted the common criteria as a part of their government procurement practices. And so while eliminating or not mandating requirements on the private sector, which we strongly discourage, they are able to ensure that the government procurement processes benefit from the best practices of the private sector.

So where are the gaps and what can government do? We would recommend four things: one is ensuring that where you are and we are creating the proper incentives for the effective implementation of the cyber security Executive Order from the White House that was issued earlier this year. That Executive Order charges the DOD and the General Service Administration, GSA, to look at ways of integrating best practices and standards from the private sector into the government procurement practices. It would be useful to create incentives to make sure that happens appropriately.

Second is your oversight power. As Mr. Dix pointed out, there are hundreds of initiatives within the public sector focused on product assurance, gaining some order and ensuring that the private sector input is integrated into those efforts is critically important.

Third is through sourcing. Ensuring that through government procurement, the government is sourcing from original equipment manufacturers and their authenticated suppliers is critical in order to have the kind of products assurance that we all have in mind.

And then fifth and final is making sure that we get an information-sharing bill similar to the one that has made its way through the House passed through the Senate as well.

Thank you very much.

[The prepared statement of Mr. Garfield follows:]

Information Technology
Industry Council

Written Testimony of

Dean C. Garfield

President & CEO, Information Technology Industry Council (ITI)

Before the

Committee on Energy and Commerce

Subcommittee on Communications and Technolgy

U.S. House of Representatives

Cybersecurity: An Examination of the Communications Supply Chain

May 21, 2013

Dean C. Garfield Testimony
Cybersecurity: An Examination of the Communications Supply Chain
May 21, 2013

Chairman Walden, Ranking Member Eshoo, and members of the subcommittee, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before the Communications and Technology Subcommittee on the important topic of cybersecurity and the communications supply chain. The Chairman and Ranking Member are well-regarded forward-thinking policy leaders on many issues that matter to our industry, and we welcome your interest and engagement on this subject.

ITI represents the world's leading technology companies from all corners of the information and communications technology (ICT) sector, including hardware, software, and services. Almost all of our members service the global market and have complex supply chains spanning multiple countries where products and services are developed, made, assembled, and distributed across the world. Supply-chain security practices are critical to our members' success—the protection of our customers, our brands, and our intellectual property are essential components of our business and our ability to grow and innovate in the future. Consequently, ITI has been a leading voice in advocating a balanced policy approach to mitigate risks and ensure the integrity of ICT supply chains.

I will focus my testimony today on four areas: (1) The considerable benefits of global supply chains to ICT companies and their customers, including the government; (2) the ICT supply-chain risks we recommend government to focus on; (3) how the private sector manages and mitigates supply-chain risks; and (4) how the government can be an effective and valuable partner in supply-chain integrity.

Ultimately our conclusion is that government has an important role to play, but government policies must be carefully calibrated to the risks faced by government or industry customers, and should not supplant the panoply of risk mitigation practices being used by ICT companies. Government policies also must be globally workable. Acting precipitously has the potential to create a check-the-box compliance regime and decrease supply-chain security over the long-run, particularly if policies regulate and mandate behavior throughout the global ICT supply chain. Unintended consequences could include deterring companies from taking swift action to respond to risk (for example, out of fear of violating a regulation that requires them to take a prescribed action when building their products), or deterring them from developing new practices to address new risks by increasing the cost of innovation.

We note that the government already is involved in a constructive way, such as by supporting global, industry-led voluntary consensus supply chain security standards activities and working with industry through the Executive Order to improve government ICT procurement practices. Greater cyber-threat information sharing is also critical—this is addressed in part in the Executive Order, but further Congressional action is needed.

Global ICT Supply Chains Benefit All Customers, Including the Government

ICT supply chains are globalized because the global system benefits all of us, including government purchasers. Most ICT acquisitions, whether made by government or industry, are fundamentally purchasing "commercial-off-the-shelf" (COTS) products. The U.S. government has a mandated preference for purchasing COTS ICT products, including for the Department of Defense. This decision was based on a calculation that in many cases the benefits to the government of using COTS hardware and software – including cost, functionality AND security – outweigh the benefits of using custom-developed products.

COTS ICT products are designed with a global audience in mind and are made available to the general public, whether individuals or organizations, and include software, such as operating systems and databases, and components and hardware, such as semiconductors, laptops, routers, and smartphones. In short, these are products we in industry and government use every day. Nearly all COTS ICT products—from U.S. and non-U.S. based companies—rely on global supply chains. By researching, developing, and manufacturing globally, COTS ICT companies gain global talent, resiliency/redundancy of suppliers, high-quality low-cost inputs, and manufacturing efficiencies. This leads to affordable, leading-edge technology products that enhance our country's productivity and competitiveness. In short, reliance on COTS rather than government-specific solutions not only cuts costs and boosts efficiency, but increases security.

It is also worth noting that, for U.S.-based companies, global supply chains have become absolutely essential to maintain a competitive edge in the global marketplace. Consumers increasingly demand 24/7/365 operations and production capacity. Global supply chains effectively keep a company's research, development, manufacturing, and maintenance of products and services operating on a 24/7/365 basis. Global supply chains are not just about company success, but also competitiveness and, therefore, survival.

ICT Industry Activities to Manage Global Supply-Chain Security Risks

Within any supply chain, as with any activity, there are risks. Risks exist during product development, manufacturing and shipment. Because these risks threaten the core of ICT businesses (our products) our sector is highly motivated to combat these risks with the same innovative focus we apply to our own product development. For ICT companies, the primary focus is the integrity, reliability and functionality of the product at hand. To advance these goals, companies assess a range of risks, including evaluating the security properties of inbound components and products as well processes and testing throughout the products lifecycle. These processes help guard against the risks of both malicious and unintentional vulnerabilities that may be inserted during the product development process.

The ICT industry manages supply-chain security risks in numerous ways. It is important to note that due to the various types of risk and their impact on such a wide variety of products in the communications sector, there is no single activity that protects all global ICT products. Instead, ICT companies utilize many different practices in concert based on an assessment of risk, which can be unique to each company's situation.

Company-specific activities: Individual ICT companies have been managing supply-chain security risks for years, and as a result, they have deep expertise on the practices that are best suited to mitigate their particular risks. Our companies undertake a number of activities to secure their supply chains.

- Product development practices. These practices span from product concept to completion. They include providing security training for product developers, defining security requirements at the outset of product development, identifying and addressing potential threats in the early design phases (e.g., threat modeling and mitigation planning), teaching and instilling secure coding practices, teaching and instilling secure code handling practices, conducting product testing to validate that security practices have been met, and security documentation.
- Purchasing from authorized suppliers, using contracts as enforcement. One way in which the technology

industry seeks to ensure supply chain integrity is through the use of authorized distributors and/or resellers. In an authorized relationship, each supplier identifies and qualifies their authorized distributors and/or resellers using a broad set of criteria, which includes legal and regulatory compliance, long-term business viability, quality systems, order placement and fulfillment processes, customer support policies, and other contractual requirements. Contracts provide enforcement mechanisms and a range of potential actions, from remediation, to termination, to legal action. In addition, suppliers periodically audit their distributors to ensure product management and contractual provisions are properly executed. Similarly, purchasing only from authorized distributors and resellers is one simple way that the U.S. government can gain higher levels of assurance than if it chooses to purchase from unauthorized sources.

Industry-wide standards activities: More recently, industry has been working together in multiple forums to develop common best practices, controls, and standards for supply-chain risk management. Several industry-wide standards and best practices address ICT supply-chain risks. Our companies contribute to developing such standards on a global, voluntary, and consensus basis through a range of organizations. Examples of supply-chain security standards include a variety of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards, including:

- ISO/IEC 15408, which serves as the basis for the Common Criteria, the global IT security certification arrangement. A pilot is underway to incorporate supply-chain risks in the Common Criteria evaluations of IT products. It is important to note that the Common Criteria is an agreement among the governments of 26 mostly developed nations. The U.S. is represented in the Common Criteria by the National Information Assurance Partnership, which is led by the National Security Agency; and
- The ISO/IEC 27000 risk management framework, which will include a component under development to address supply-chain security (27036, information security for supplier security).

In addition, other activities include:

- The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.
- The Open Group Trusted Technology Forum (OTTF) is an industry-led global standards initiative that aims to shape global procurement strategies and best practices that help to reduce threats and vulnerabilities in the global supply chain. The U.S. Department of Defense is a member of the OTTF.
- SAE-AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" is an industry best practice.

The standards efforts above are global, with participation and contributions from companies from all over the world. In addition, many of them include government participation—not as dominant players, but as distinct stakeholders with interests in the outcome.

Again, it is important to stress there is no one-size-fits-all "supply-chain security standard" or set of practices applicable across the board. The security practices a particular company chooses depend on its products, services, markets, and business methods. In addition, industry continually updates existing standards or establishes new standardization efforts addressing emerging cybersecurity risk concerns. Thus, the government should recognize and support these activities, but not mandate any one standard, approach, or activity. Such an inflexible approach would likely divert resources away from addressing emerging risks and challenges, thereby decreasing security. Given the substantial time and resources the government would need to devote to identifying standards and writing them into contracts, the reality is that any government –required standards will be static, rather than evolving to address changing threats. Security standards evolve as new threats and vulnerabilities emerge, and new products and technologies emerge as well. *Today's best practice can be outdated tomorrow.*

How the Government Can Be Helpful

As policymakers, you are increasingly and rightfully interested in the security of the software and hardware procured by government agencies and critical infrastructure (CI) sectors generally. This increased government focus is putting new expectations on industry's supply-chain risk management activities. The single largest thing that government can do to address its concerns regarding government systems is ensure that all ICT products are purchased from authorized sources.

In recent years we have seen a rush to legislation and regulation, and to interfere with standards development. There have been dozens of supply-chain related bills and provisions in legislation, including in successive National Defense Authorization Acts, and most recently, in the continuing funding resolution that was enacted just last month. More are expected. Various agencies, including the Department of Defense, the Department of Homeland Security, the National Institute of Standards and Technology, the Office of Management and Budget, the General Services Administration, and the Department of Commerce are working on proposals and programs alone or at an interagency level to address supply-chain concerns.

We support the government's efforts to better understand and improve the security of U.S. federal and telecommunications systems and networks. We consider ourselves partners in this shared effort. We certainly understand the urge to act as fast as possible, but also believe an important rule to follow is based on the old adage "first, do no harm." That starts with ensuring that proposed solutions to perceived supply-chain security concerns are based on sound risk management practices. In addition, we believe the best solutions are ones that acknowledge the global nature of supply chains and therefore work in concert with the sophisticated processes and procedures industry has been implementing for decades.

Some recent proposals, however, have tended to:

- Insist on a regulatory system;
- Include U.S. Government-specific requirements or approaches (such as new standards written by the government for industry-wide use);
- Not allow for private-sector leadership and collaboration;
- Include technology mandates that artificially pick winners and losers;
- Include burdensome procurement requirements that go beyond federal procurement and into mandates on industry;
- Focus solely on vendors' design and building of products, and not on government users' procurement and implementation;

- Focus on specific supply-chain vulnerabilities, and not supply-chain risk management; and
- Focus on where technology is developed, rather than how, which fails to evaluate the security of the product, gives a false sense of security, and is incompatible with global supply-chain models.

Most concerning is that many of these proposals have the unintended consequence of decreasing, not increasing, cybersecurity, because industry needs the flexibility to innovate in response to actual and emerging threats. U.S.-specific regulations and practices could impede U.S.-based ICT companies' ability to compete in the global marketplace. For example, measures that would require companies to build U.S.-specific products, in addition to products for the global market, would have an immeasurable negative competitive impact. Second, other countries, interpreting our actions as an attempt to create barriers to foreign entry into U.S. markets, will emulate such proposals and pursue their own domestic requirements. A "race to the bottom" of a myriad of national requirements would ensue, leading to a patchwork of conflicting requirements from various governments, balkanizing the global ICT marketplace. This would significantly diminish the benefits that our customers derive from our massive research and development (R&D) investments – which we can only afford if we can expect the commensurate return on investment that comes from serving a global marketplace. These benefits include fast paced innovation (new products with new and useful features), global interoperability, low cost, and – most importantly – constantly improved product security.

Unfortunately, we are already seeing other countries propose market access restrictions under a banner of supply-chain security. We fear a contagion effect from these types of approaches that will undermine U.S. cybersecurity and U.S.-based company success in global markets.

U.S. government efforts should focus on:

- Creating incentives for the effective implementation of the President's February 12 cybersecurity Executive Order to continue. The Executive Order directs the General Services Administration and the Department of Defense to study the merits of incorporating global, industry-led cybersecurity standards into federal acquisition planning and contract administration. The ICT industry is deeply committed to improving cybersecurity and, as such, we are deeply involved in this work and want to make it a success.
- Ensuring private sector participation in the supply-chain work within the Executive branch. As with any cybersecurity issue, public-private partnerships are critical. Currently there are various supply-chain efforts within the Administration. Although it has been challenging at times for the private sector to have input into that work, now both the IT Sector Coordinating Council and Communications Sector Coordinating Council have active supply-chain committees that are working closely with DHS and other government agencies to jointly review this work.
- Sourcing technology from authorized sellers and resellers. Federal purchasers and their contractors should procure ICT equipment directly from original equipment manufacturers (OEMs) or their authorized resellers and service partners, except when the item is discontinued or otherwise unavailable. This can help to minimize the chances that counterfeit or tainted products will be unintentionally acquired, mitigating a significant risk to government supply chain. Too often, we have seen government agencies procure technology products from companies that had no relationship with the products manufacturers, and had themselves bought the products from unverified sellers.
- Passing effective cyber threat information-sharing legislation.

I want to highlight this last point. There is a very important role the government can play in partnership with industry. Effective sharing of actionable information among and between the public and private sectors about cyber threats and incidents is an essential component of improving cybersecurity—including in ICT supply chains. We know from experience that once effectively informed of the specific threats they face, organizations take appropriate and reasonable measures to mitigate them. The Executive Order intends to improve the government's sharing of actionable information with the private sector on specific, targeted cyber threats and technical indicators that flag risks generally. We hope these changes are executed quickly but we also believe Congress can build on the EO by addressing liability concerns that impede information flows. That is why ITI supports the Cybersecurity Intelligence Sharing and Protection Act, which received strong, bipartisan support in the House a few weeks ago. We are working with legislators to continue to improve this bill. We support Senate efforts to adopt a corresponding bill and will push this legislation towards enactment in this Congress.

Government efforts should also preserve the ability of our members' private sector customers, including the telecommunications industry, to leverage our members' compliance with global industry-led standards and best practices. The government has long recognized that taking a light touch approach to regulating the telecommunications industry has fostered innovation and competition, to the benefit of the American consumer. The results are clear. The U.S. now leads the world in fourth generation long-term evolution (4G LTE) deployment, with as many subscribers in this country as there are throughout the rest of the world. In terms of wired broadband, today 80 percent of U.S. households have access to networks capable of 100 megabit speeds. And all the while, the communications industry has been consistently cited as one of the leading sectors in cybersecurity. We encourage Congress to continue this light-touch approach when looking at the communications supply chain and thereby, to enable industry to respond to evolving threats with innovation, flexibility, and the most updated and appropriate global standards and best practices.

Conclusion

Members of the subcommittee, ITI and our member companies are pleased you are looking at how we can improve supply-chain security. As I said at the opening of my testimony, supply-chain security is absolutely critical to our members' success. The protection of our customers here and around the world, our brands, and our intellectual property are essential components of our business and our ability to grow and innovate in the future. We stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that mitigate risks and ensure the integrity of ICT supply chains. Thank you.

Mr. LATTA. Thank you, Mr. Garfield, for your testimony. And, Mr. Chair, do you want to resume the chair?

Mr. WALDEN. Or I can just ask questions from here if you want to wield that big gavel there.

Mr. LATTA. Yes. Well, with that then the vice chair will recognize the chairman of the subcommittee for his 5 minutes of questions.

Mr. WALDEN. Thank you, sir, and thanks for filling in and getting the hearing going back from the votes. I got detained, as occasionally happens on the floor.

Mr. Garfield—first of all, thank you to all of our witnesses—but I appreciated your comments. Our networks and the threats they face are varied, as you know, and they are ever-changing, as you reference in your testimony. So how do we secure our supply chain without losing the flexibility that is critical to both how our communication networks function and then how to defend them? What do you recommend here?

Mr. GARFIELD. You put your finger on the idea of the point of drawing balance. I think building on the best practices that are being developed in the private sector and integrating those into the government procurement efforts. There are a number of standards-based initiatives that are moving forward, specifically focused on product assurance in supply chains. And so I would strongly encourage taking advantage of those best practices and integrating them into our government procurement practice.

Mr. WALDEN. You know, I have another question here that plays on this a bit for Ms. Bisceglie and Mr. Baker and you, Mr. Garfield. Sometimes it appears the government sort of has an ad hoc process if you will when it comes to protecting the supply chain. A high-ranking official will place a call or write a little letter to a company suggesting that the company not do business with a particular vendor or a particular piece of equipment. I have actually had experience with that with a constituent. So do we need a more formalized process, which raises all kinds of questions as to who is making those decisions and all, but both as a matter of good process for equipment buyers and sellers to ensure that the measures are effective? And then how would you formalize that process?

And I don't want to hobble, you know, the fast-paced communications industry with a lot of bureaucracy, and red tape, and approval processes either. We fight that in other sectors and you certainly don't want it here. And it gets back to the hearings that we held that said, you know, first do no harm in this area. Bad guys will get ahead of us and we will be locked into old laws and rules. So is there a way to strike a balance here? And what do you recommend?

Ms. BISCEGLIE. I am happy to go first.

So I do agree we need to have—I think it is a separate slippery slope——

Mr. WALDEN. Yes.

Ms. BISCEGLIE [continuing]. As you just mentioned. And I think that there are different levels. There is a varied way to put in a formalized process and I personally believe or we personally believe there is no one-size-fits-all, but we like to talk about frameworks.

Mr. WALDEN. Right.

Ms. BISCEGLIE. And that framework consists of training and awareness, which I talked about earlier——

Mr. WALDEN. Right.

Ms. BISCEGLIE [continuing]. Which is a very big thing. Folks need to understand what the risk is that we are all talking about.

Mr. WALDEN. Right.

Ms. BISCEGLIE. Additionally, I think that the thing that we have seen over the last 6 years is that organizations, both public and private, really struggle with understanding their internal risk tolerance. So how much risk can I actually accept into my organization——

Mr. WALDEN. Like anything else.

Ms. BISCEGLIE [continuing]. And that is not necessarily a single risk number of 1 to 5. It can be based on the essential function of that organization and if it has multiple functions, then it gets prioritized, if you will, into the different programs that that organization conducts as well as the systems that support that. And then underneath that, I think you do have some sort of a formal process. It gets really simple to us and that it really goes back to just really good business practices and understanding who you are buying from.

Mr. WALDEN. Right.

Ms. BISCEGLIE. But unless you can look at an organization and understand where their vulnerabilities exist and have a process to go through that, I think it is a very difficult place to go. I do think that that last-minute, that 3:00 a.m. phone call is again a very dangerous place to be.

Mr. WALDEN. Mr. Baker?

Mr. BAKER. So I completely agree we can't just start regulating——

Mr. WALDEN. Right.

Mr. BAKER [continuing]. The private sector and tell them how to do this. At the same time, if we rely exclusively on the government communicating informally about its concerns, you run the risk that the people who want to make these sales will just keep lowering the price and lowering the price.

Mr. WALDEN. Right, we have seen that.

Mr. BAKER. Hard to resist. And so I would suggest that there needs to be authority for the government at a minimum to ask questions. What is in your supply chain?

Mr. WALDEN. Right.

Mr. BAKER. You know, what products are you buying? And to communicate where they have a strong basis, that is not acceptable. We know enough to know that that is a risky place to buy your equipment, so don't do it.

Mr. WALDEN. I will show a little ignorance here, but is there sort of a range of equipment in the system that there is some that is more important to make sure you get right than others, or is it just everything matters?

Mr. BAKER. There is a view abroad and in the industry as well in telecommunications that the core is your most important product——

Mr. WALDEN. Right.

Mr. BAKER [continuing]. And you cannot compromise the core and that the edge is less risky because fewer people are——

Mr. WALDEN. Do you agree with that?

Mr. BAKER [continuing]. For any particular system. I am not sure in an internet world as the edge gets smarter and smarter that that is a distinction that holds up as well as we would like it to. But that is certainly something that we have seen in other telecommunications decision-making.

Mr. WALDEN. I know Mr. Garfield didn't get a chance to respond but I also know my time has run out so—yes, you have got to watch this vice chair. He is mean with that gavel. Do you have anything to add to that, Mr. Garfield?

Mr. GARFIELD. I do. I think there are two specific processes——

Mr. WALDEN. Yes.

Mr. GARFIELD [continuing]. That would be useful. One is a process that is being set up through CISPA if it is passed through the Senate——

Mr. WALDEN. Right.

Mr. GARFIELD [continuing]. Which is a formal process for information-sharing through the government with the protections necessary to make sure that information-sharing takes place.

The second is that the Executive Order sets up a process through the Department of Defense and General Service Administration. And so creating ways to incentivize the success of that, which Congress can still do, I think is critically important.

Mr. WALDEN. All right. Thank you very much and I yield back the deficit balance of my time.

Mr. LATTA. The chairman is so recognized. The chair now recognizes the gentlelady from California and the ranking member, Ms. Eshoo, for 5 minutes.

Ms. ESHOO. Thank you, Mr. Chairman. It is nice to see you in the chairman seat, and you are always a gentleman and I appreciate that.

Mr. WALDEN. Reserving the right to object.

Ms. ESHOO. Well, the same applies to you Mr. Chairman. The same applies to you. Not to worry, not to worry. Thank you to all the witnesses. Let's see, two, four, six, seven people have, you know, each in your own way have come in with something that has some refinement to it that helps to not necessarily bring closure but get us to focus on the areas that are really important for us to focus on when it comes to a public role of national security and the integrity of the supply chain. So I thank you.

I have a lot of questions. Let me start with—and Mr. Lindquist is probably not going to be surprised with the Electronic Warfare Associates, that is quite a name. Warfare Associates. How about Peace-fare Associates? But I guess that doesn't work as well. Now, I understand that your company vetted Huawei's equipment and you gave it your seal of approval. I might add that the more I have heard witnesses speak, the more I think the government really needs to have some kind of list of essentially a good housekeeping seal of approval on it because small companies especially really need to have some help and direction so that they are not caught in some kind of seamless web.

But can you explain the service you provided Huawei and what ongoing monitoring you have conducted to maintain your certainty that their equipment is safe to use? And did Huawei pay you for this? And, I mean, if they did, you know, I don't know where that places the veracity of the report. I mean, it could be—I am not saying that is—but it could be the equivalent of what happened on Wall Street when the rating agencies were paid to give some of these, you know, too-big-to-fail great, great ratings. But they paid for them. And so, you know, in the aftermath and the rubble of the aftermath, that didn't sound so good. It didn't feel so good and really wreaked a lot of havoc. Did Huawei pay you for the report? And then the rest of my question.

Mr. LINDQUIST. First of all no, Huawei did not pay for——

Ms. ESHOO. You did this voluntarily for them?

Mr. LINDQUIST. No, the telecommunications carrier paid for it.

Ms. ESHOO. And who was that?

Mr. LINDQUIST. I am not at liberty to disclose that because we have an NDA with them. If I get their permission, I can tell you easily who it is.

Ms. ESHOO. I see. That is interesting.

Mr. LINDQUIST. But it is one of the major——

Ms. ESHOO. Yes.

Mr. LINDQUIST [continuing]. Telecommunications companies. And——

Ms. ESHOO. An American telecommunications company?

Mr. LINDQUIST. American telecommunications company.

Ms. ESHOO. Yes.

Mr. LINDQUIST. Secondly——

Ms. ESHOO. Can you tell us this? Is it an American telecommunications company that buys equipment from Huawei?

Mr. LINDQUIST. They are in the process of doing that. The equipment, in answer the second part of your question——

Ms. ESHOO. Yes.

Mr. LINDQUIST [continuing]. We are in the process of evaluating their system. The evaluation is by no means complete and we are only evaluating the radio area network portion of it. There are numerous reports. We do not give a seal of approval. What we do is take the known threats and we have very good access through some of our work within the government to the agreed list of cyber threats and what——

Ms. ESHOO. Well, do you get your information from the intelligence community or Homeland Security?

Mr. LINDQUIST. The intelligence community.

Ms. ESHOO. This is so interesting. So you do a report that vets Huawei, who wants to more than get a toehold which have for years and it is very public and deeply concerned about. You are paid by an American major telecommunications corporation that is looking to buy Huawei's equipment and you work with the intelligence community to see with the shortfalls are and vet it and say that the equipment is terrific for the American market. Have I gotten that straight?

Mr. LINDQUIST. Well, except that we don't say it is terrific or——

Ms. ESHOO. What did you say?

Mr. LINDQUIST. What we do say is what we looked at and what we found, and if we found things, what corrections were made.

Ms. ESHOO. I see. See, my issue on all of this is not whether their equipment is good or not. That is not the point. The point is that our infrastructure is so precious to this country and it is a part of our national security. There is no question about it. And so does it pose a threat? If so, how? You know, maybe they make some of the best equipment in the world but that is not my point. That is not my point at all. So it is interesting what you just said.

And let me ask all the witnesses and you can just give me a yes or no. Should there be transparency requirements, including divestments in state ownership placed on companies seeking to sell telecommunications infrastructure equipment to U.S. network providers? And should this be a U.S. or an international standard? Maybe it is hard to answer yes or no but——

Mr. GOLDSTEIN. I don't think I can give you a yes or no, ma'am. I think, particularly from our perspective, we didn't look at those issues specifically. It is something we are happy to talk to staff about.

Ms. ESHOO. I want to thank you for your work, too.

Mr. GOLDSTEIN. Thank you.

Ms. ESHOO. Yes.

Mr. BAKER. I do think that as we adjust to a world where there really are no telecommunications integrators in the United States, we need authority to ask for quite a bit of information from the people——

Ms. ESHOO. Yes.

Mr. BAKER [continuing]. Who are supplying that technology.

Ms. ESHOO. Thank you.

Ms. BISCEGLIE. I absolutely agree. I think transparency is the key and you liken it to—if you look at what is happening with the pharmaceutical agencies within your actual State——

Ms. ESHOO. Yes.

Ms. BISCEGLIE [continuing]. That the pharmaceutical law, the E-Pedigree law of 2015 that has everybody looking at transparency, I think there are lessons to be learned there.

Ms. ESHOO. Yes. OK.

Mr. DIX. Transparency is important and having a standard that provides certification and accreditation like a whitelisting type of opportunity would be very valuable to this process.

Ms. ESHOO. Thank you.

Mr. ROTHENSTEIN. Yes, we would agree. We would support some level of transparency and I think, frankly, Ranking Member Eshoo, you hit the nail on the head. It is less about the U.S. Government and about the large service providers who have a lot of know-how——

Ms. ESHOO. Yes.

Mr. ROTHENSTEIN [continuing]. The resources, and are knowing smart buyers of telecom equipment understand the risks. It is more about other critical infrastructure owners and operators, the alternative operators, the enterprises who may not have the same level of understanding and resources where the transparency really is going to be important.

Ms. ESHOO. It is helpful. Yes.

Mr. LINDQUIST. As I said earlier, I would reiterate transparency is important. That is why in the process that we implement we are looking at all the design documentation behind the various systems to ensure that there is no inexplicable capability or functionality within the system.

Mr. GARFIELD. I work in the tech sector so, of course, we believe in transparency. I don't have an answer as it relates specifically to this issue.

Ms. ESHOO. Thank you. Thank you, Mr. Chairman, for your patience. Thank you to all the witnesses.

Mr. LATTA. Thank you very much. The gentlelady yields back and the chair recognizes himself now for 5 minutes.

And if I could start with Mr. Goldstein, I found it kind of interesting in your testimony on page 5 where you state that other countries such as Australia, India, and the United Kingdom are similarly concerned about emerging threats to the commercial communication networks posed by the global supply chain, have taken actions to improve their ability to address this security challenge. What exactly have those three countries done?

Mr. GOLDSTEIN. There are three countries—there are many others——

Mr. LATTA. Right.

Mr. GOLDSTEIN [continuing]. That we don't get into here. But Australia has developed a regulatory reform proposal that they expect to put in place shortly that would allow the government to have more authority to examine what companies are doing, what they are buying, how they document their purchases, take a look to make sure that those companies are competent in putting networks together, and if the government does not feel that they are doing it in a way that can be secured, that they can ask them to do more. They can require them to do more than they are doing and it has enforcement powers and potential to find those companies that don't do it. That is a proposal that is likely to pass soon.

India has a very similar reform program in place. Where it differs is that they have also proposed requiring—certainly encouraging and in many cases requiring much of their equipment to be made and tested in the country and could not be obtained elsewhere. That particular part of the proposal has been put on hold because the United States and some other countries have objected because of potential barriers to trade.

And the United Kingdom has put in place a very similar program to the one that Australia is now contemplating to have a greater regulatory review over the practices and actions of companies putting networks in place, which also has authorities for them to go in and look very specifically at what they have done and how they are going to get assurance that those are secure networks, as well as to be able to enforce actions that they feel would be necessary if those companies did not do as much as they probably should be doing.

Mr. LATTA. Thank you.

Mr. Rothenstein, if I could turn to your written testimony. I thought it kind of interesting where you had also had mentioned that in 2011 your company had made a conscious decision to gradually exit key elements of your supply chain from China. And at the time over 1/5 of your global chain at that time originated in China. You go on to state that, you know, you are looking at other jurisdictions that you are moving into now in Mexico and Thailand. I am just curious. How is that working out, and what have you found so far with that transition?

Mr. ROTHENSTEIN. So in terms of the actual specific—so you are right. About 20 percent at the time of our manufacturing assembly of our supply chain originated in China and it is now down to less than 1 percent. And in terms of the procurement to finished to semi-finished assemblies, that was about 65 to 70 percent of the supply chain 2 years ago. That is now below 50 percent. The part that we attacked, as I mentioned in my testimony, was that relating to active or programmable components.

In terms of how it has gone, it has gone very, very well. We have partnered effectively with two of our long-standing contract manufacturers in Mexico and one in Thailand. We have improved the velocity of our supply chain. It is a lot quicker to get equipment to our key North American market when you are driving it by truck over the border as opposed to the slow boat from China. We have been able to essentially achieve cost parity in terms of labor rates and landed cost rates largely because those contract manufacturers had existing facilities in those locations.

And as a result of that, we have been able to, in addition to velocity maintaining cost parity, we have gotten tremendous positive feedback from our customer base in terms of that supply chain strategy. They viewed very positively our thought process, our decision, and they have given us direct feedback that they view with a greater level of comfort, security, and assuredness of the risk profile of our equipment to their networks.

Mr. LATTA. And in the balance of my last 27 seconds if I could turn to Mr. Lindquist, what are the different challenges in protecting the software and hardware supply chain and is one more vulnerable than the other?

Mr. LINDQUIST. What are the different challenges in protecting it?

Mr. LATTA. In protecting the software and hardware supply chains and is one more vulnerable than the other?

Mr. LINDQUIST. I think the current state of affairs—and it is referring to the second question first—I think the software is more vulnerable. I think there are more people who have perfected techniques for exploiting software than in the hardware. It is also easier to do at any stage in the process.

And what we are endeavoring to do is to separate the vendor from the products so that once the system has been determined to be secure enough, and there is always some residual risk, that the vendor no longer has access to that system to introduce any new malicious capability into the system.

Mr. LATTA. Well, thank you very much. And my time has expired.

And the chair would now recognize the gentleman from Illinois, Mr. Shimkus, for 5 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman. Thank you all for being here. It is a great committee with high-tech things. I always joke that for my colleagues who don't have teenagers, then the government ought to issue them one because that helps you figure out how this stuff works.

The hearing this morning was on cyber security, too, with the electric grid and the like. So we had a little debate about the cloud, which I understand are server farms and that brings some, especially when the government is contracting. And my son and I are together on concerns about the cloud. You know, everybody thinks it is—but, you know, there are some issues there, cyber security and especially if the government is being involved and really contracting that space.

We differ on CISPA and we have had numerous debates. So the last time we cast the vote I was home that next morning and he comes into the room and he is all grouchy and he is reading all of his internet stuff. And he says I don't have to ask how you voted on CISPA, Dad. I know how you voted—which I supported. And he was none too pleased.

But my debate or discussion with him is information-sharing, really on the code system so you could have firewalls. And if our intel communities or you guys know something is crazy going on out there, you can build a firewall. At least you have an idea of what you might expect.

So, Mr. Garfield, I don't know if it was in your statement but in question-and-answers you also talked about information-sharing. And were you referring to that in the supply chain debate that we are having here, that there ought to be information-sharing like we would have in firewall protection a la like CISPA?

Mr. GARFIELD. Yes is the simple answer. Information-sharing and passing of risk mitigation information is critical to protecting our cyber security generally but also for risk assurance in the context of supply chains as well. And so, I think, moving CISPA and the information components of that was critically important and getting it through the Senate is critically important——

Mr. SHIMKUS. But the CISPA bill that we are passing—you know, correct me if I am wrong—I thought it was just on code. Was it also on the supply chain? It could be?

Mr. GARFIELD. Yes, it is around sharing actionable intelligence——

Mr. SHIMKUS. Here on——

Mr. GARFIELD [continuing]. On threats and mitigating threats.

Mr. SHIMKUS. I got another good point for my son then, right? I got another good point.

Mr. GARFIELD. You can give him my phone number.

Mr. SHIMKUS. Good. Great. Good, I always need a little help.

And Ms. Bisceglie, SCRM, now, I have got a new acronym. Just what we need, another acronym here in Washington, SCRM, which was supply chain——

Ms. BISCEGLIE. Risk management.

Mr. SHIMKUS [continuing]. Risk management, which is all tied into this. I want to follow up with you on this cost pressure issue that you raised and how do you think we can really address it? I mean if you really want to make sure that your equipment is secure, you are willing to pay for it, but if you are in a competitive, very fast-moving technological field and you want to get market entry and you want to have a low-cost provider, there is risk involved in that, correct?

Ms. BISCEGLIE. There is, and actually, that is when the chairman asked his question earlier when we talked about putting a framework in place, something that is repeatable and scalable. I personally think that is the key, an effort to keep the acquisition costs down, because I totally understand the need to get procurements done faster, technology to the street faster, and into users' hands faster. But unless we have ways of understanding what our organizational risk tolerance is so that we know what protectionisms we already have in place, it is going to be very difficult to really take risky endeavors like you are mentioning.

Mr. SHIMKUS. And I was also caught by the whole debate. There was a pharmaceutical reference which we are involved with and the Track-and-Trace legislation——

Ms. BISCEGLIE. Yes.

Mr. SHIMKUS [continuing]. In maybe some States. Just for the record, when some States move to a very controlled system, they have to then postpone the enactment date because they can't do it——

Ms. BISCEGLIE. Yes.

Mr. SHIMKUS [continuing]. In that time, which then would affect the market in delivery of goods and services. So the question is—because what the chairman said to begin with was, first do no harm.

Ms. BISCEGLIE. Yes.

Mr. SHIMKUS. So does the Executive Order and its process have the opportunity to do harm in this process? Does anyone want to comment? Is there a concern that the Executive Order and this rollout and their involvement has an opportunity to do harm? Mr. Garfield?

Mr. GARFIELD. Yes, there is always risk, right? We are in the business of risk mitigation but overall our view is that the Executive Order actually creates a framework that advances the ball in a very positive way. The fundamental question for us is how can Congress complement that and that is what I tried to articulate in talking about the things that Congress can do to ensure it continues to move in a positive direction.

Mr. SHIMKUS. Mr. Chairman, my time is up but I think there are a couple more that want to comment.

Mr. DIX. I would just add many of us want to approach the answer to that question with an open mind, but we are taking a wait-and-see approach because it is not at the endgame yet and there are opportunities along the way for this not to be as good as it might be.

Mr. SHIMKUS. Always good to trust but verify.

Mr. DIX. Yes, sir.

Mr. SHIMKUS. If no one else wants to jump in, I yield back my time. Thank you, Mr. Chairman.

Mr. WALDEN. Thank you. Now, I will turn to the gentleman from Colorado, Mr. Gardner, for 5 minutes.

Mr. GARDNER. Thank you, Mr. Chairman, and thank you to the witnesses for joining us today.

And, Mr. Baker, I will direct this question to you. Questions raised by foreign-directed cyber attacks on U.S. institutions suggest that the United States Government must give careful consideration to how the national security interests are controlled, monitored, and regulated. How concerned should we be by the prospect that any critical infrastructure provider that serves the core of our national security interests could come under foreign control and therefore outside the supervision of the U.S. Government?

Mr. BAKER. We have to be concerned about that. It is not likely that we will be able to stop globalization of this industry so the idea that we can simply say no I think is not realistic. But we have to then put in place transparency and regulatory authority that makes sure that those companies do not serve other nations' interests when they supply us with that equipment.

Mr. GARDNER. And in keeping those kinds of concerns in mind—and we have seen in the past the mergers of U.S. companies with foreign companies—what are some of the national security implications of such a purchase then?

Mr. BAKER. So I did this a lot when I was at DHS and indeed when I was at NSA. In the telecommunications industry we have a well-developed set of rules in which we negotiate a mitigation agreement with the buyer if the buyer is a foreign buyer, which gives us some control. It is not perfect by any means, and I am often unenthusiastic about the results. But it is the tool that we have.

In the context of companies selling products to the United States, we have none of those controls unless they actually buy a U.S. company so that any company can sell products into our critical infrastructure without any regulation or transparency. It is only when they try to buy a U.S. company that we have any authority at all.

Mr. GARDNER. Reports of stories of foreign-directed cyber attacks against U.S. institutions provoke difficult questions about the control reaching oversight of the United States national security interests. Do you agree that the idea of surrendering control of a critical infrastructure provider like Sprint to a foreign entity Softbank beyond full U.S. oversight deserves very careful consideration and should not be hurried?

Mr. BAKER. It certainly deserves careful consideration. I would point out, as I answered to the last question, for many the security agencies there will be a temptation to say the only way we will be able to tell Sprint the products they can buy, what they can have in their infrastructure, is if we enter into a negotiated agreement. That is a negotiated agreement with a foreign buyer. They have no authority at all in the other context so it is an odd set, currently, of incentives for the U.S. Government in which they might actually have more regulatory authority if they let the transaction go through.

Mr. GARDNER. You mentioned in your testimony a little bit about CFIUS, whether it is adequate or not. That is relied on by Congress, by the FCC. Where are the pitfalls? What are the problems?

Mr. BAKER. The problem is that if you want to introduce products that are not reliable into the U.S. market, you can just walk in and start taking orders. Even if it is going right into the core of the telecommunications industry, there is no authority anywhere in the U.S. Government to say no to that today. Only if an unreliable buyer or seller actually tries to acquire a U.S. company is there any authority at all.

Team Telecom at the FCC has some authority over foreign carriers but not over foreign suppliers of equipment. CFIUS gives authority only over buyers of U.S. companies. So there is a real regulatory gap there with respect to some of this equipment that we have not yet found a solution for.

Mr. GARFIELD. May I weigh in on this?

Mr. GARDNER. Please.

Mr. GARFIELD. I think we have to be exceptionally careful about developing prophylactic rules around private sector agreements as it relates to supply chain assurances. India was used as a reference earlier in talking about an example of countries moving in a particular direction. There are a whole host of companies that I represent in the technology sector that are being foreclosed from the Indian market because of those types of rules. And so I just think that those types of rules have to be carefully calibrated and, from my perspective, discouraged.

Mr. GARDNER. Thank you. I yield back my time.

Mr. WALDEN. I thank the gentleman. I thank all of our witnesses and committee members for their participation today, really a superb panel of witnesses. Your information that you shared has been very, very valuable. Your written testimony is helpful to us and to our staffs as we wrestle with this issue going forward in protecting the country and trying also not to stifle innovation and technology being developed in America. So we have got to get this right. And your depths of experience and your willingness to come here and share that with us is a great benefit to the American people. And so we thank you for your participation; we thank you for your assistance.

And the record will remain open for additional questions, I am sure. And we hope that you will accept our invitation to work with us even further as we go forward. We want to get this right. So thank you very much. With that, the Subcommittee stands adjourned.

[Whereupon, at 4:12 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. FRED UPTON

Wired and wireless technologies are increasingly becoming the medium over which we manage our lives, our government, and our country. As a result, national security, economic security, and personal security are now also matters of communications security. Where once it may have been sufficient to guard the doors to our homes, our banks, our offices, our factories, and our utilities, today we must also guard the virtual doors to our networks.

This hearing will look at the locks we place on those networks throughout the communications supply chain. Just as the networks and the cyber threats they confront are varied and ever evolving, so too must be our defenses. A one-size-fits-all solution is likely to be as successful as fitting every lock with the same key.

What means are at the disposal of the private sector and government to secure our networks? What's working? What isn't? Where are the threats coming from? What kind of risk and cost-benefit analyses should we be engaging in to find the right solutions? I ask the witnesses to help frame the issues for us today so we can determine where we-and the nation-should focus attention. If no one watches the door, surely someone will walk in who shouldn't.

# # #

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

October 3, 2013

Mr. Mark L. Goldstein
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Goldstein:

Thank you for appearing before the Subcommittee on Communications and Technology on May 21, 2013, to testify at the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, October 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Charlotte.Savercool@mail.house.gov and mailed to Charlotte Savercool, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

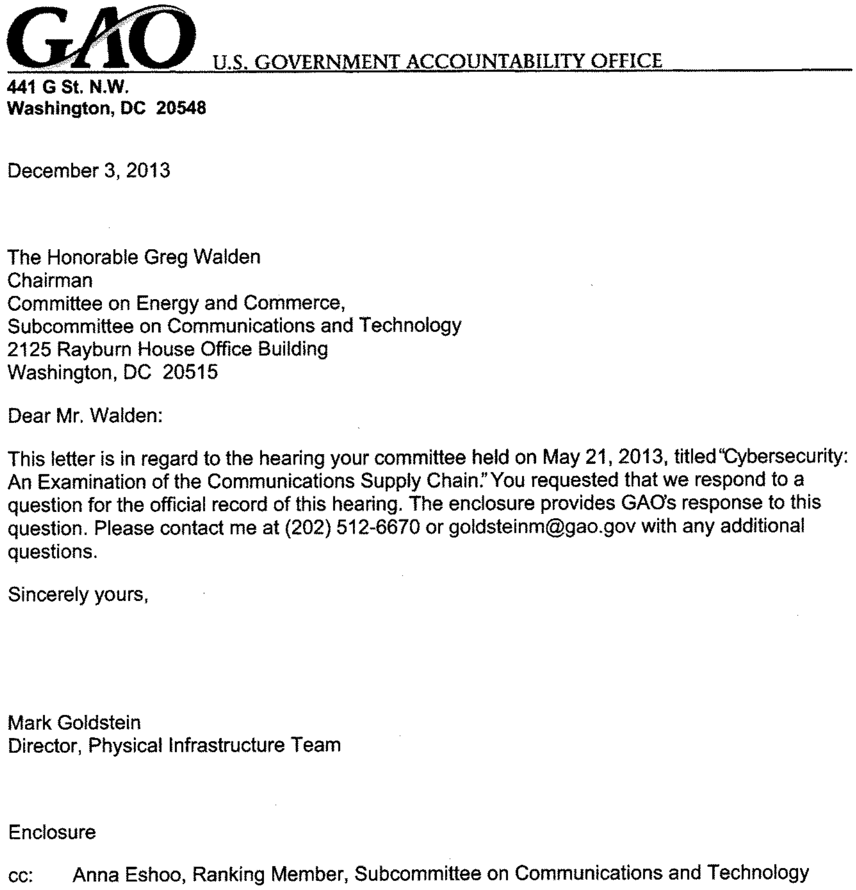
Sincerely,

Greg Walden

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment



GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

December 3, 2013

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce,
Subcommittee on Communications and Technology
2125 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Walden:

This letter is in regard to the hearing your committee held on May 21, 2013, titled“Cybersecurity: An Examination of the Communications Supply Chain.”You requested that we respond to a question for the official record of this hearing. The enclosure provides GAO’s response to this question. Please contact me at (202) 512-6670 or goldsteinm@gao.gov with any additional questions.

Sincerely yours,

Mark Goldstein
Director, Physical Infrastructure Team

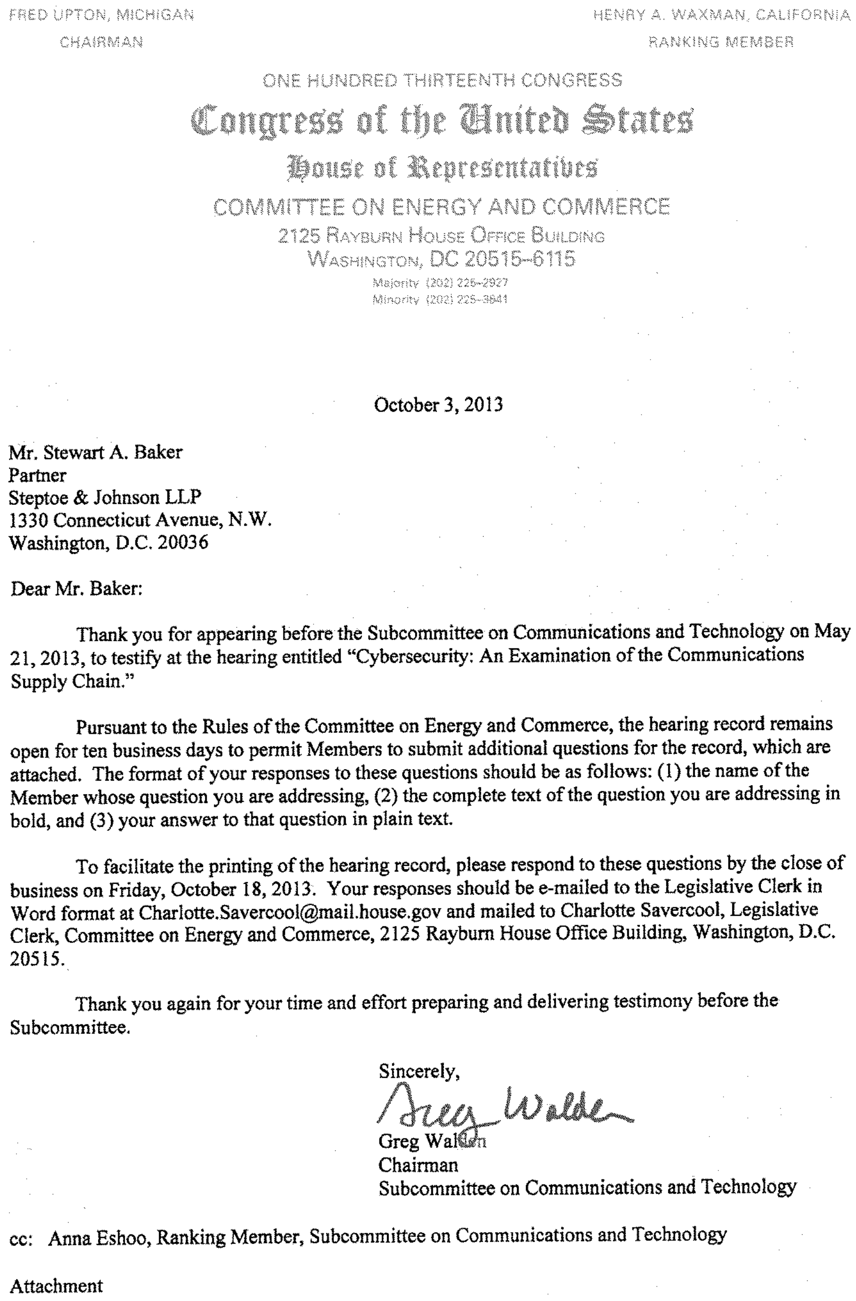
Enclosure

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

The Honorable Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

The GAO's report explores the concept of expanding the U.S. Government's Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-made equipment. The report notes a series of concerns that could result such as trade barriers, additional costs, and constraints on competition. Do you believe the benefits outweigh the drawbacks of expanding the CFIUS review process?

GAO is not making a judgment as to whether the benefits of expanding the CFIUS process outweigh the drawbacks. As stated in the May testimony, discussions between the Communications Sector Coordinating Council and participating federal entities on adapting a CFIUS type voluntary notification process for use on equipment purchases were, at the time, ongoing, and it is not clear how the proposal will develop, if at all. The council is trying to understand the threats the government is concerned about and whether these could be best addressed by a CFIUS-type process or some other means.



FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

October 3, 2013

Mr. Stewart A. Baker
Partner
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036

Dear Mr. Baker:

Thank you for appearing before the Subcommittee on Communications and Technology on May 21, 2013, to testify at the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, October 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Charlotte.Savercool@mail.house.gov and mailed to Charlotte Savercool, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Walden

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment

Cybersecurity: An Examination of the Communications Supply Chain
Before the Committee on Energy and Commerce
Subcommittee on Communications and Technology
U.S. House of Representatives
Hearing Held: May 21, 2013

Response to Questions For The Record From The Honorable Anna Eshoo
By Stewart A. Baker
Partner, Steptoe & Johnson LLP
Former Assistant Secretary for Policy, Department of Homeland Security
Former General Counsel, National Security Agency

Question 1:

The GAO's report explores the concept of expanding the U.S. government's Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-manufactured equipment. The report notes a series of concerns that could result such as trade barriers, additional costs, and constraints on competition. Do you believe the benefits outweigh the drawbacks of expanding the CFIUS review process?

Response:

CFIUS and Team Telecom already have broad authority, and they seem to have exercised that authority already to set limits on foreign manufactured equipment in the Sprint case. Before expanding CFIUS's authority we should make sure that the change is actually necessary.

Question 2:

Should the FCC review procurements of foreign equipment by U.S. companies operating on our telecommunications networks?

Response:

The FCC currently does not have any explicit authority to regulate the purchase of foreign equipment by US companies. It does, however, seem clear that the largest carriers are currently paying close attention to the US government's concerns in that area. So continuing to voice those concerns may at least be a good starting point.

Question 3:

To what extent does our nation's intelligence community work with the FCC to assess threats to our telecommunications infrastructure?

Response:

The FCC has a generally cooperative relationship with the intelligence and defense communities. That is in large part due to the deference the FCC pays to Team Telecom as the representative of US national security interests in telecom infrastructure. The deference in my experience has been quite genuine and cooperative, despite the lack of a statutory requirement.

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 Rayburn House Office Building
Washington, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

October 3, 2013

Ms. Jennifer Bisceglie
President and CEO
Interos Solutions, Inc.
8200 Greensboro Drive, Suite 900
McLean, VA 22102

Dear Ms. Bisceglie:

Thank you for appearing before the Subcommittee on Communications and Technology on May 21, 2013, to testify at the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, October 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Charlotte.Savercool@mail.house.gov and mailed to Charlotte Savercool, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

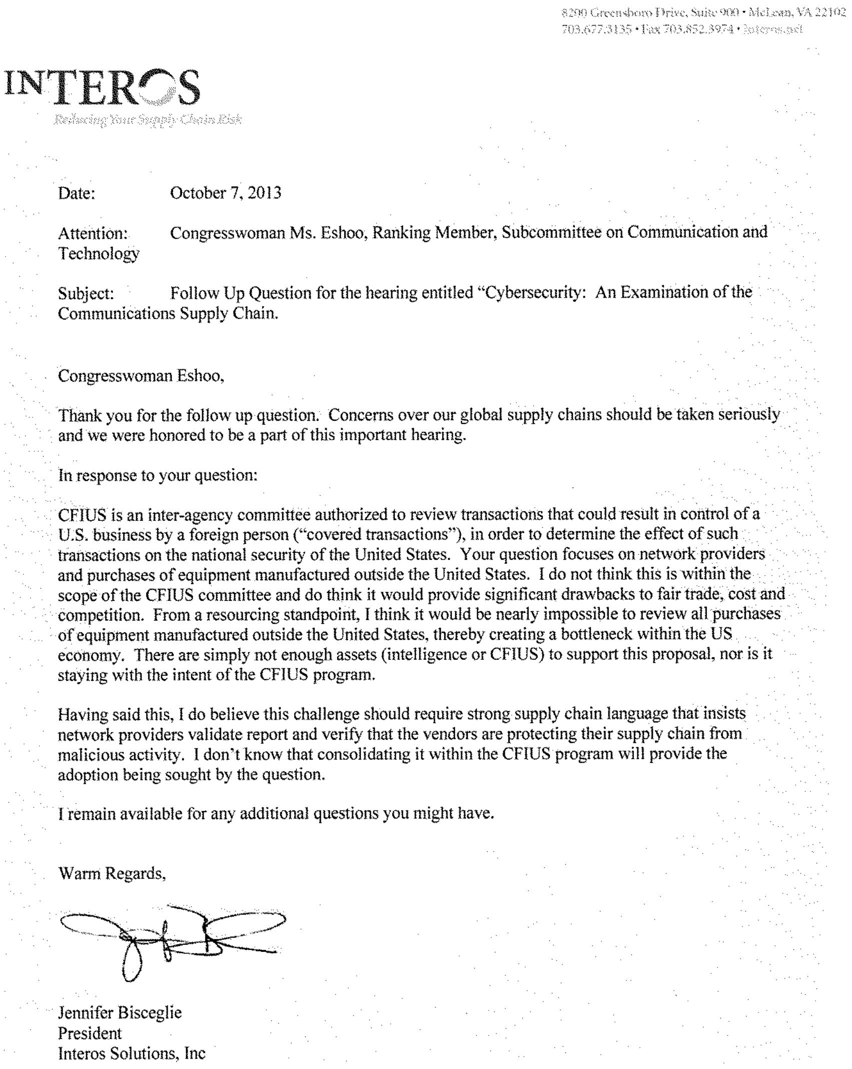
Sincerely,

Greg Walden

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment



8290 Greensboro Drive, Suite 900 • McLean, VA 22102
703.677.3135 • Fax 703.852.3974 • interos.net

INTEROS
Reducing Your Supply Chain Risk

Date: October 7, 2013

Attention: Congresswoman Ms. Eshoo, Ranking Member, Subcommittee on Communication and Technology

Subject: Follow Up Question for the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain.

Congresswoman Eshoo,

Thank you for the follow up question. Concerns over our global supply chains should be taken seriously and we were honored to be a part of this important hearing.

In response to your question:

CFIUS is an inter-agency committee authorized to review transactions that could result in control of a U.S. business by a foreign person ("covered transactions"), in order to determine the effect of such transactions on the national security of the United States. Your question focuses on network providers and purchases of equipment manufactured outside the United States. I do not think this is within the scope of the CFIUS committee and do think it would provide significant drawbacks to fair trade, cost and competition. From a resourcing standpoint, I think it would be nearly impossible to review all purchases of equipment manufactured outside the United States, thereby creating a bottleneck within the US economy. There are simply not enough assets (intelligence or CFIUS) to support this proposal, nor is it staying with the intent of the CFIUS program.

Having said this, I do believe this challenge should require strong supply chain language that insists network providers validate report and verify that the vendors are protecting their supply chain from malicious activity. I don't know that consolidating it within the CFIUS program will provide the adoption being sought by the question.

I remain available for any additional questions you might have.

Warm Regards,

Jennifer Bisceglie
President
Interos Solutions, Inc

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

October 3, 2013

Mr. Robert B. Dix, Jr.
Vice President
Government Affairs and Critical Infrastructure Protection
Juniper Networks
2251 Corporate Park Drive, Suite 200
Herndon, VA 20170

Dear Mr. Dix:

Thank you for appearing before the Subcommittee on Communications and Technology on May 21, 2013, to testify at the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, October 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Charlotte.Savercool@mail.house.gov and mailed to Charlotte Savercool, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

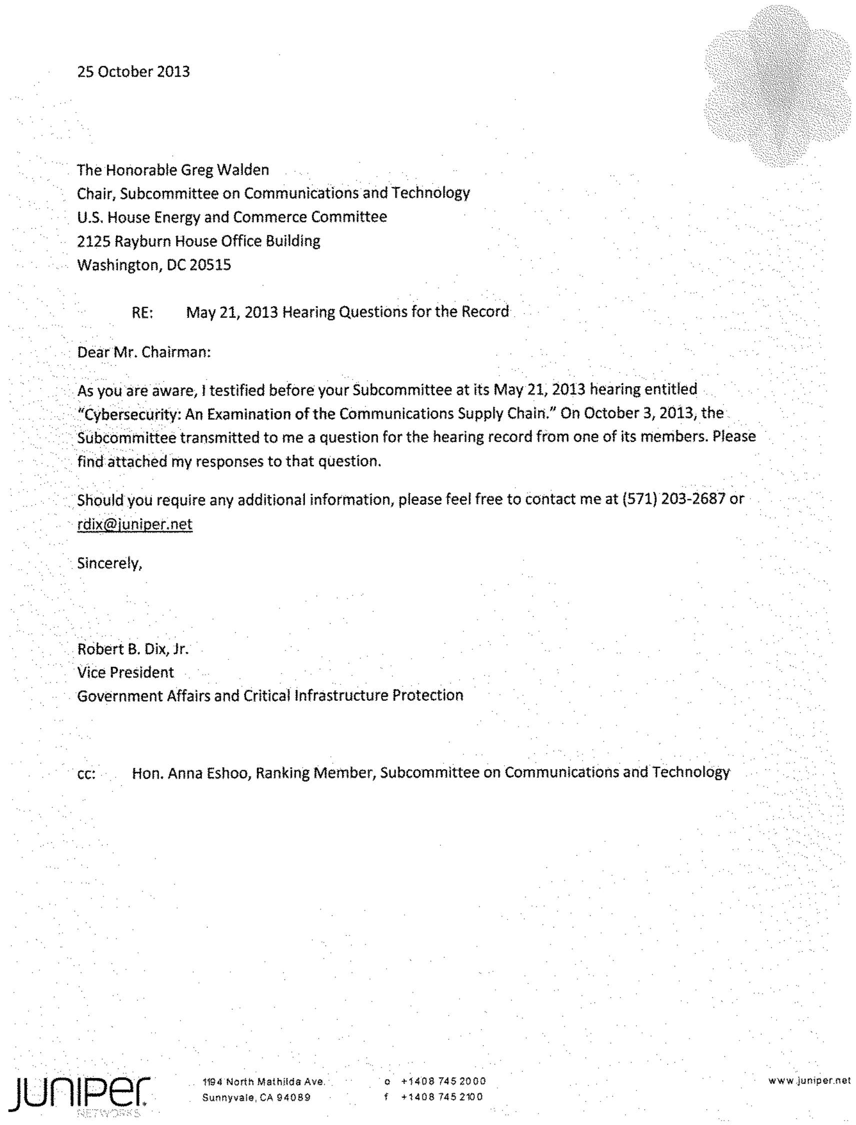
Sincerely,

Greg Walden

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment



25 October 2013

The Honorable Greg Walden
Chair, Subcommittee on Communications and Technology
U.S. House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

RE: May 21, 2013 Hearing Questions for the Record

Dear Mr. Chairman:

As you are aware, I testified before your Subcommittee at its May 21, 2013 hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain." On October 3, 2013, the Subcommittee transmitted to me a question for the hearing record from one of its members. Please find attached my responses to that question.

Should you require any additional information, please feel free to contact me at (571) 203-2687 or rdix@juniper.net

Sincerely,

Robert B. Dix, Jr.
Vice President
Government Affairs and Critical Infrastructure Protection

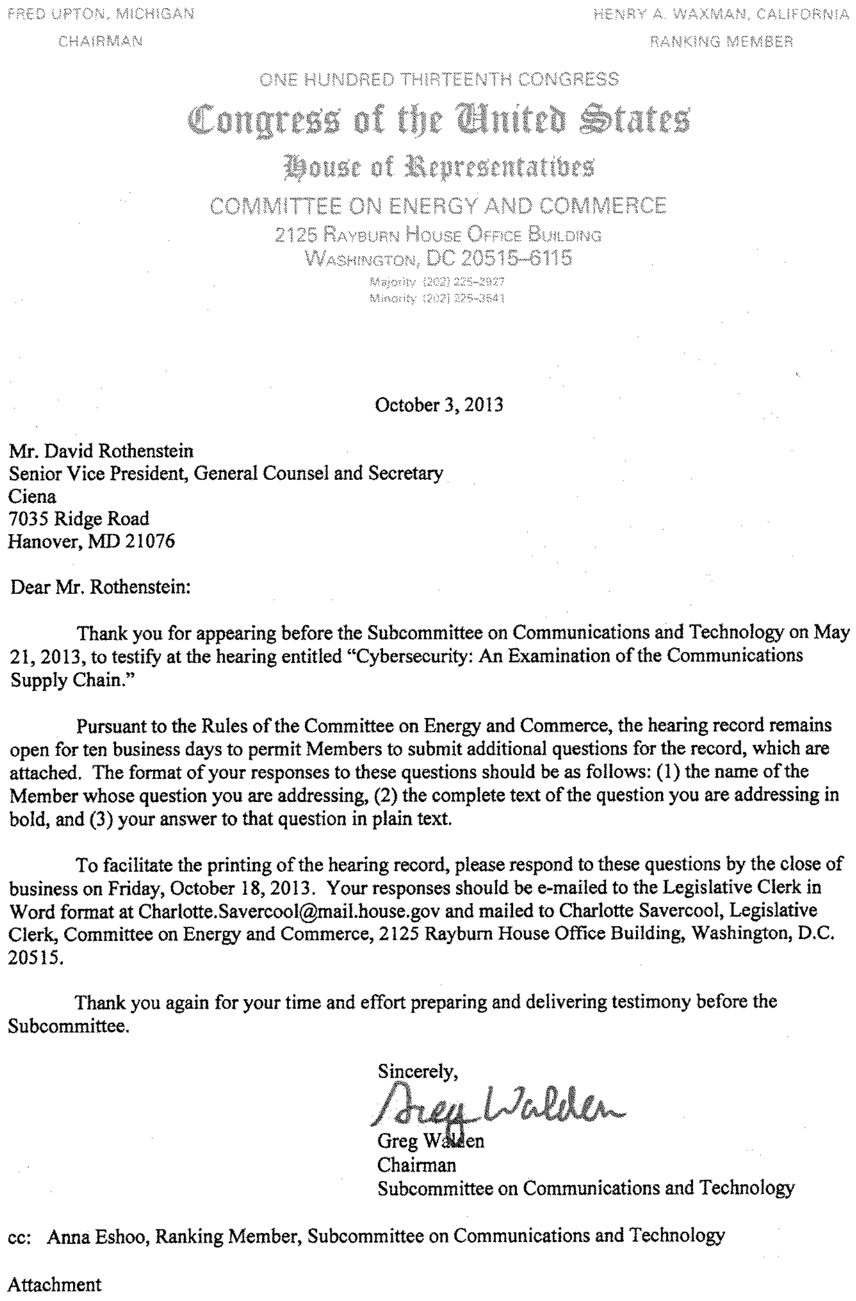
cc: Hon. Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

QUESTIONS FOR THE RECORD
Robert B. Dix, Jr., Juniper Networks
House Subcommittee on Communications and Technology
May 21, 2013

QUESTION POSED BY THE HONORABLE ANNA ESHOO

1. The GAO's report explores the concept of expanding the U.S. government's Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-manufactured equipment. The report notes a series of concerns that could result such as trade barriers, additional costs, and constraints on competition. Do you believe the benefits outweigh the drawbacks of expanding the CFIUS review process?

Ranking Member Eshoo, thank you for seeking Juniper Networks's input on this important issue. In our view, the advantages and disadvantages of an expanded CFIUS process would depend on exactly how it was structured and for what types of transactions. With respect to the U.S. government supply chain, Juniper supports the idea that U.S. departments and agencies should be permitted to purchase information and communications technology, including hardware and software, from only authorized and trusted sources. As a network or system becomes less critical, it is not abundantly clear that there is a significant benefit to a costly CFIUS process.



FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

October 3, 2013

Mr. David Rothenstein
Senior Vice President, General Counsel and Secretary
Ciena
7035 Ridge Road
Hanover, MD 21076

Dear Mr. Rothenstein:

Thank you for appearing before the Subcommittee on Communications and Technology on May 21, 2013, to testify at the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, October 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Charlotte.Savercool@mail.house.gov and mailed to Charlotte Savercool, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Walden

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment

ciena

7035 Ridge Road
Hanover, Maryland 21076-1425

410 694 4500 phone
410 865 8001 fax

[illegible]

January 17, 2014

The Honorable Anna Eshoo
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Question:

The GAO's report explores the concept of expanding the U.S. government's Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-manufactured equipment. The report notes a series of concerns that could result such as trade barriers, additional costs, and constraints on competition. Do you believe the benefits outweigh the drawbacks of expanding the CFIUS review process?

Answer:

As part of our public policy advocacy efforts over the past several years, Ciena Corporation has given significant consideration to the role that CFIUS could play in network provider purchases of foreign-manufactured equipment. In our view, if the proposed expansion of the CFIUS review process were appropriately defined and tailored to adequately address the concerns set forth below and in the GAO report, then we believe that the benefits could potentially outweigh the drawbacks. If that were not the case, however, then we believe that the drawbacks would outweigh the benefits of expanding the CFIUS review process.

In order to make an effective assessment of any CFIUS expansion, Ciena believes that policymakers must consider the following:

1. Network providers have varying level of sophistication when it comes to testing and evaluating communications networking equipment. In our experience, some providers – typically the largest carriers and U.S. government agencies – have a deep understanding of and appreciation for the security benefits that are derived from our efforts to move our supply chain out of China. However, there are many private sector enterprise buyers of networking equipment that simply do not have the same level of sophistication or understanding of the security risks posed by equipment in their networks, or the same infrastructure resources with which to test and evaluate such equipment. Because some of these enterprises run enormous global networks, they may be unintentionally creating significant risks to their companies, customers and employees. In many cases, however, their networks are just as critical to our nation's well-being. At the same time, the scope of and breadth of network equipment today is quite significant. Not all network equipment functions in the same manner, operates in the same place in a network, or poses the same risks to security of the network. Accordingly, from a policy perspective, in order that the review net is

appropriately tailored to the relative risk posed by the transaction, there should be meaningful consideration given to the definitions of both "network provider" and "purchases" for purposes of triggering potential CFIUS review.

2. Under the current structure of the telecommunications industry supply chain, the vast majority of communications networking equipment – including equipment marketed and sold by Ciena – incorporates at least some components or subcomponents that are manufactured in a foreign country. As a result, broad policy proscriptions relating to "foreign-manufactured equipment" could theoretically impact every equipment purchase by network providers, which is not, in our view, the right policy approach. Instead, we believe that a more appropriate and practical approach would be to expand the CFIUS review to purchases of foreign-manufactured networking equipment from a subset of companies that may have interests adverse to those of the United States, both from a national security and a trade and economic perspective.

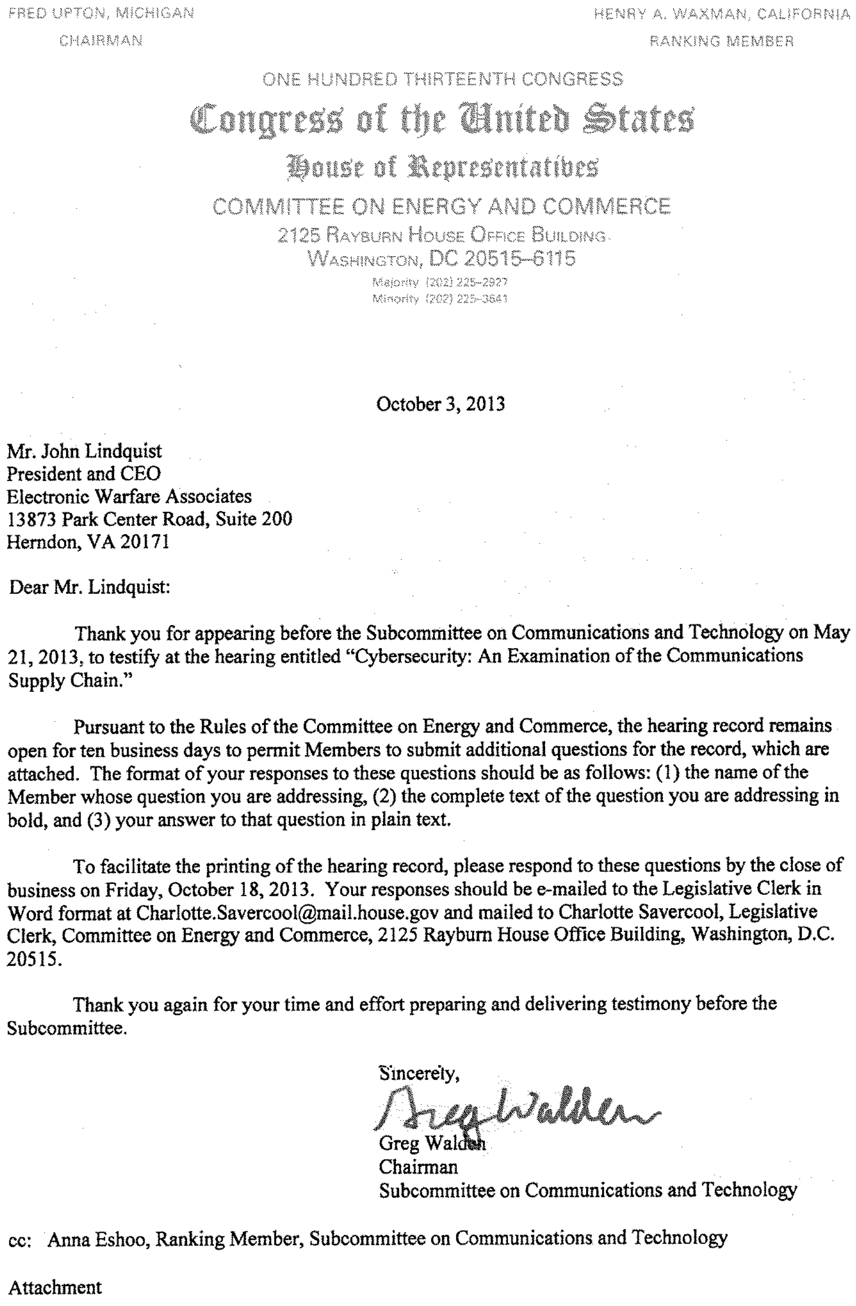
3. In light of the rapid transition of the communications industry to "software-defined networking" and "network function virtualization," the importance of software to current and future networks cannot be understated and is absolutely critical from a product integrity and product assurance perspective. By way of example, we have implemented strict controls over our software development, and the final testing and validation all of the software loaded onto our products is performed in North America. In so doing, we reduce the risk that the software can be tampered with or modified and thereby create network security concerns for our customers. Therefore, to the extent that any review process is created for network provider purchases of equipment, it must necessarily consider the integrity of the embedded software and any application software, where it installed, by whom, as well as who will conduct ongoing and routine maintenance and support of the software.

As a result of the above, Ciena continues to believe that the most important next step is a broad-based education program for enterprise purchasers of network equipment, particularly those enterprises with critical infrastructure. It would certainly be in the economic and security interest of the United States to find a way to routinely share information such entities so that they make more informed buying decisions.

Sincerely,

On behalf of Ciena Corporation

David M. Rothenstein
Senior Vice President and General Counsel



FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congreſs of the United States

House of Repreſentatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

October 3, 2013

Mr. John Lindquist
President and CEO
Electronic Warfare Associates
13873 Park Center Road, Suite 200
Herndon, VA 20171

Dear Mr. Lindquist:

Thank you for appearing before the Subcommittee on Communications and Technology on May 21, 2013, to testify at the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, October 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Charlotte.Savercool@mail.house.gov and mailed to Charlotte Savercool, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Walden

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment

Mr. John Lindquist
President and CEO
Electronic Warfare Associates
13873 Park Center Road, Suite 200
Herndon, VA 20171

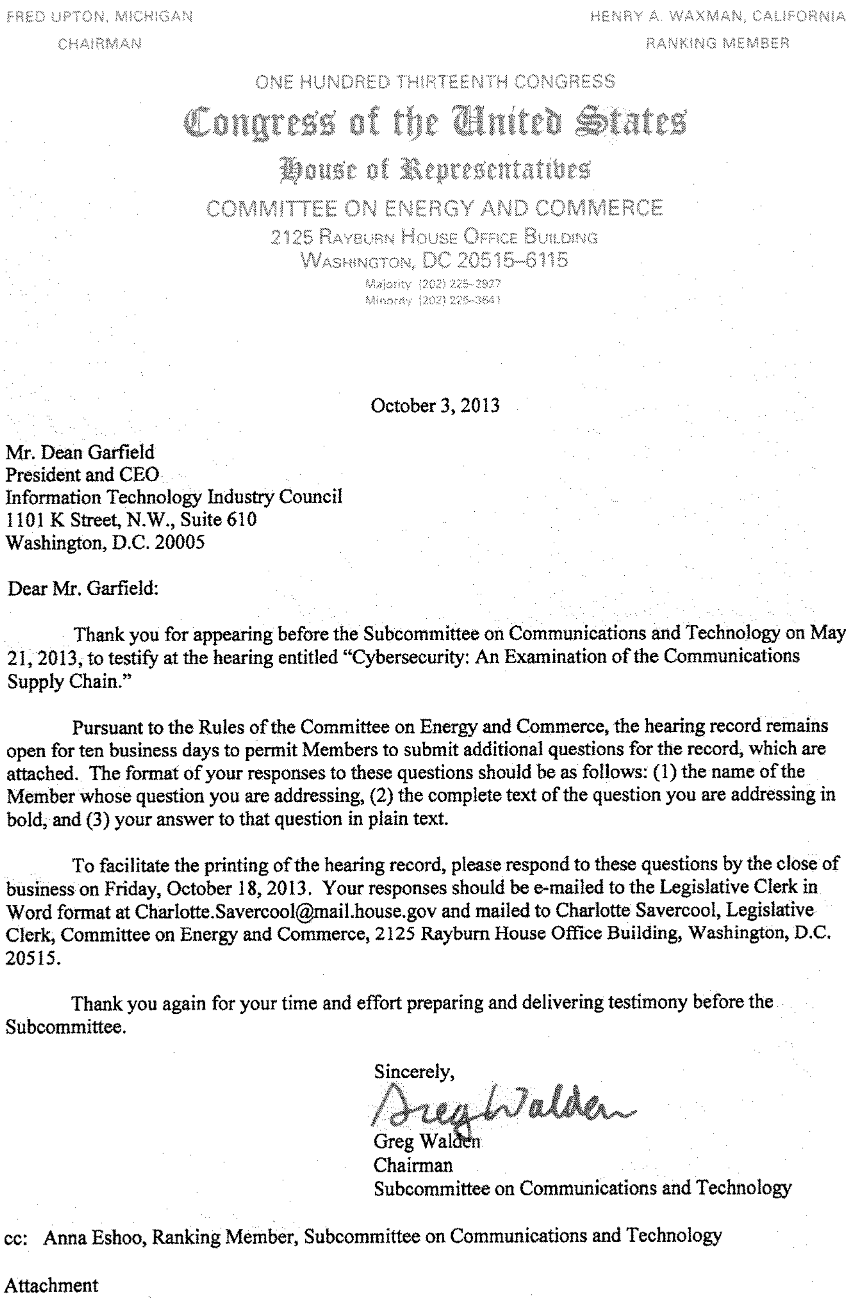
The Honorable Anna Eshoo

The GAO's report explores the concept of expanding the U.S. government's Committee On Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign manufactured equipmet. The report notes a series of concerns that could result such as trade barriers, additional costs, and constraints on competition. Do you believe the benefits outweigh the drawbacks of expanding the CFIUS review process?

Expanding the Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-manufactured systems will be significantly burdensome on all concerned because there are no manufacturers of telecommunications equipment in the United States. Furthermore, the bulk of the components (board level and below as well as software and firmware) integrated into telecommunication systems are also manufactured outside the United States. More to the point, all manufacturers of telecommunications equipment, including software and firmware, have significant developmental and production facilities in the Peoples Republic of China as well as other nations that, from time to time, might find it in their interest to subvert or disrupt U.S. networks. In light of the global nature of the network providers supply chain, CFIUS would be in a position of evaluating the entire supply chain on a continuous basis. That becomes extremely difficult because the pedigree of the components and software routines used in the systems are often extremely difficult, if not impossible to determine which in turn makes it very difficult to assess the risk associated with the components and, therefore the risk to the system.

The CFIUS review process is designed to determine who can be trusted. The nature of the supply chain makes it nearly impossible to know who was involved in the development and manufacture of a network system or its components. If one can't know who is involved, one can't know who to trust.

A more productive, and less disruptive approach, would be to develop an independent review process, similar to the process put forth in a recent CFIUS mitigation agreement. The agreement requires a detailed analysis of hardware, firmware, and software so as to provide an acceptable level of assurance that the system is free of components and subcomponents designed or corrupted to enable malicious exploitation. In addition, the agreement requires a trusted delivery process that ensures that the system delivered is exactly the same as the system evaluated. The result is that the network provider, and in turn the U.S. government, can decide whether or not to trust the system based empirical evidence rather than on the country in which the manufacturer has located its headquarters. Since all components have a great likelihood of manufacture outside the U.S. by non-U.S companies, it might serve the Committee's goals more effectively, to review the High Assurance Analysis and Trusted Delivery Processes as well as the Independent Evaluator implementing those processes. This approach would limit the complexity of the CIFIUS Review Process, and avoid many of the feared trade economic and political drawbacks, and dramatically increase the security posture of the network system.



FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

October 3, 2013

Mr. Dean Garfield
President and CEO
Information Technology Industry Council
1101 K Street, N.W., Suite 610
Washington, D.C. 20005

Dear Mr. Garfield:

Thank you for appearing before the Subcommittee on Communications and Technology on May 21, 2013, to testify at the hearing entitled "Cybersecurity: An Examination of the Communications Supply Chain."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Friday, October 18, 2013. Your responses should be e-mailed to the Legislative Clerk in Word format at Charlotte.Savercool@mail.house.gov and mailed to Charlotte Savercool, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Greg Walden

Greg Walden
Chairman
Subcommittee on Communications and Technology

cc: Anna Eshoo, Ranking Member, Subcommittee on Communications and Technology

Attachment

Information Technology
Industry Council
Innovation. Insight. Influence.

Question received from the Honorable Anna Eshoo, U.S. House of Representatives:

> *The GAO's report explores the concept of expanding the U.S. government's Committee on Foreign Investment in the United States (CFIUS) review process to include network provider purchases of foreign-manufactured equipment. The report notes a series of concerns that could result such as trade barriers, additional costs, and constraints on competition. Do you believe the benefits outweigh the drawbacks of expanding the CFIUS review process?*

Answer: No. ITI believes expanding CFIUS in this regard has numerous drawbacks that might outweigh any benefits. We concur with the findings in the May 2013 GAO report[1] that such an approach could result in trade barriers, additional costs, and constraints on competition. Such an approach also could negatively impact the security of U.S. communications networks.

Expanding CFIUS as proposed will decrease, not increase, security. The proposal is based on an incorrect premise that security is a function of where network equipment is manufactured and that equipment manufactured in a foreign country is inherently less secure. Product security is a function of how a product is designed, engineered, and maintained, not where it is manufactured. If forced to manufacture in a given country, companies lose significant flexibility to innovate in response to actual and emerging threats. A focus on where technology is developed, rather than how, fails to evaluate the actual security of the product and can lull buyers into a false sense of security. The global ICT industry encourages all governments to refrain from enacting policies that discriminate based on technologies' country of origin.[2]

Secondly, this proposal would impact nearly every information and communications technology vendor, including U.S.-headquartered ones, since nearly all network equipment is manufactured in foreign countries. By researching, developing, and manufacturing globally, companies gain global talent, resiliency/redundancy of suppliers, high-quality low-cost inputs, and manufacturing efficiencies. This leads to the affordable, leading-edge technology products, with the high level of security demanded by businesses, governments, and consumers. Thus, harms we foresee, enumerated below, will fall on U.S. and foreign companies alike.

Expanding CFIUS as proposed would harm our companies' competitiveness and trade. Other countries, interpreting our actions as an attempt to create barriers to foreign entry into U.S. markets, will emulate such proposals and pursue their own domestic requirements. A "race to the bottom" of such requirements would ensue, leading to a patchwork of conflicting

[1] GAO, "Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment," May 21, 2013.

[2] "Global ICT Industry Statement: Recommended Government Approaches to Cybersecurity," DIGITALEUROPE, ITI, and JEITA, June 2012, p. 2. ***Reconfirm title and insert footnote***

requirements from various governments, balkanizing the global ICT marketplace. This would significantly diminish the benefits—fast-paced innovation (new products with new and useful features), global interoperability, low cost, and constantly improved product security—that derive from our massive research and development (R&D) investments which we can only afford if we can serve a global marketplace. Being able to innovate in this regard is essential to our companies' survival. In fact, a recent Brookings report noted that government policies enacted in the name of "cybersecurity" could, if they are country-specific, impede the global flow of information technology products and services, harming information technology firms and vendors as well as importing countries.[3]

Unfortunately, we are already seeing other countries going down the path proposed. The most egregious cases include India and China. India's 2012 Preferential Market Access policy aims to impose domestic manufacturing requirements on telecommunications equipment sold in the commercial market. While China has long sought to keep foreign ICT products out of its market, recent China-focused policies coming out of Washington have increased motivation behind these exclusionary policies. Changing CFIUS as contemplated will be seen as a retaliatory measure towards Chinese companies, spurring China to move forward on its plans to set up a CFIUS-like Review Commission.

In addition to India and China, Indonesia, Nigeria, and other countries have domestic technology procurement requirements on the books. U.S. industry is working with the Administration to push back on these restrictions and our successes depend in part on being able to state that such approaches deviate from global norms. If the U.S. government begins to review commercial communications transactions, we will lose much of our bargaining power, which could result in foreign markets increasingly shut to our companies.

Expanding CFIUS to commercial transactions also would be extremely costly and unwieldy. As described by GAO (pp. 9-10), communications networks in the United States are highly complex. Multiple network providers operate distinct regional and other smaller networks, including wireless, wireline, and cable access segments, which interconnect to a national backbone to form a national infrastructure. The entire network relies on hundreds if not thousands of types of products. Further, as GAO also highlights (p. 37), network providers conduct thousands of transactions a year. These purchases may serve to update one portion of a regional network, or be part of a phased-in national upgrade. It would be very time-consuming for both providers and vendors to file a CFIUS report on each of these transactions, a likely scenario given that each transaction would include foreign-manufactured equipment. In addition, detailing the country in

[3] Friedman, Allan, "Cybersecurity and Trade: National Policies, Global and Local Consequences," Brookings Institution Center for Technology Innovation, September 2013.

http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookingscybersecuritynew.pdf which certain equipment is manufactured could be impossible from the vendor perspective. As described above, vendors have global supply chains. Further, vendors constantly change their

sources of supply, based factors such as price. This would hamper any ability to cite prior filings related to the same type of equipment.

Mandating a review of each commercial transaction also would overwhelm the CFIUS process, which was not designed for that type of capacity. The number of CFIUS cases now averages from 100-200 per year.[4] Changing the CFIUS scope would result in a substantial—not marginal—increase in workload. This in turn is likely to lengthen the average review time, which at a minimum 30-75 days[5] already is quite long. Such a delay would raise costs for network providers, equipment vendors, and, ultimately, U.S. consumers (also pointed out by GAO, p. 36). It also would delay the roll-out of 4G LTE and other leading-edge networks in the United States, hampering the efficiency and productivity all U.S. businesses and consumers, and the U.S. government, enjoy from our communications networks. And these benefits translate into a significant impact on U.S. competitiveness and growth. Last year, Ericsson, Arthur D. Little, and Chalmers University of Technology, concluded that for every 10 percentage point increase in broadband penetration GDP increases by 1 percent.

In 2012, GAO released a separate report in which federal officials from the Director of National Intelligence (DNI), NSA, and the CIA provided reasons why the cost of tracking IT equipment's country of origin outweighed the potential benefits.[6] That report was focused on government procurement, but if these agencies feel that country-of-origin tracking was not a benefit for their own procurements, it is doubtful tracking for commercial telecommunications network purchases would be any more useful.

Both my May 2013 testimony (pp. 3-5) and the May 2013 GAO report (pp. 15-27) list a range of steps industry, network providers and equipment vendors, and the government are taking to address cyber-related risks in U.S. communications networks. U.S. government efforts should focus on:

- Creating incentives for the effective implementation of the President's February 12 cybersecurity Executive Order to continue. The Executive Order directs the General Services Administration and the Department of Defense to study the merits of incorporating global, industry-led cybersecurity standards into federal acquisition planning and contract administration. The ICT industry is deeply committed to improving

[4] ***(need footnote from Treasury website)***
[5] CFIUS includes a mandatory 30-day review, and CFIUS may institute a subsequent 45-day investigation (which can be extended). In addition, parties need time to get a filing complete before submitting it.

[6] GAO, IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," March 2012, p. 27.

cybersecurity and, as such, we are deeply involved in this work and want to make it a success.

- Ensuring private sector participation in the supply-chain work within the Executive branch. As with any cybersecurity issue, public-private partnerships are critical. Currently

  there are various supply-chain efforts within the Administration. Although it has been challenging at times for the private sector to have input into that work, now both the IT Sector Coordinating Council and Communications Sector Coordinating Council have active supply-chain committees that are working closely with DHS and other government agencies to jointly review this work.

- Sourcing technology from authorized sellers and resellers. Federal purchasers and their contractors should procure ICT equipment directly from original equipment manufacturers (OEMs) or their authorized resellers and service partners, except when the item is discontinued or otherwise unavailable. This can help to minimize the chances that counterfeit or tainted products will be unintentionally acquired, mitigating a significant risk to government supply chain. Too often, we have seen government agencies procure technology products from companies that had no relationship with the products manufacturers, and had themselves bought the products from unverified sellers.

- Passing effective cyber threat information-sharing legislation.

These approaches are commendable and should be encouraged. Expanding CFIUS as proposed would hamper, not help, these activities and would negatively impact security, trade, innovation, and competitiveness as described above.